Part No. 209570-B
September 2001

4401 Great America Parkway
Santa Clara, CA 95054

Using Web-based Management for the Business Policy Switch 2000 Software Version 1.2

NORTEL NETWORKS™

Copyright © 2001 Nortel Networks

All rights reserved. September 2001.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Autotopology, BaySecure, BayStack, Business Policy Switch, Nortel Networks, the Nortel Networks logo, and Optivity are trademarks of Nortel Networks.

Internet Explorer, Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Acrobat and Adobe are registered trademarks of Adobe Systems Incorporated.

Netscape Navigator is a registered trademark of Netscape Communications Corporation.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

Nortel Networks NA Inc. software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks NA Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS

AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface 21

Before you begin 21
Text conventions 22
Related publications 22
How to get help 23

Chapter 1
Using the Web-based management interface 25

New features 25
Stacking compatibility 26
Software version 1.2 compatibility with BayStack 450 switches 27
Requirements 28
Port numbering syntax 29
Logging in to the Web-based management interface 29
Web page layout 30
    Menu 31
    Management page 34

Chapter 2
Administering the switch 37

Viewing system information 38
Configuring system security 39
    Setting console, Telnet, and Web passwords 39
    Configuring RADIUS security 41
Logging on to the management interface 42
Resetting the BPS 2000 43
Resetting the BPS 2000 to system defaults 44
Logging out of the management interface 45

Chapter 3
Viewing summary information 47

Viewing stack information 47
Viewing summary switch information 49
Viewing switch information in real time 51
Changing stack numbering 54
Identifying unit numbers 56

Chapter 4
Configuring the switch 57

Configuring BootP, IP, and gateway settings 58
Modifying system settings 60
About SNMP 61
Configuring SNMPv1 62
Configuring SNMPv3 63
    Viewing SNMPv3 system information 63
    Configuring user access to SNMPv3 65
        Creating an SNMPv3 system user configuration 65
        Deleting an SNMPv3 system user configuration 68
    Configuring an SNMPv3 system user group membership 68
        Mapping an SNMPv3 system user to a group 68
        Deleting an SNMPv3 group membership configuration 70
    Configuring SNMPv3 group access rights 71
        Creating an SNMPv3 group access rights configuration 71
        Deleting an SNMPv3 group access rights configuration 72
    Configuring an SNMPv3 management information view 73
        Creating an SNMPv3 management information view configuration 73
        Deleting an SNMPv3 management information view configuration 75
    Configuring an SNMPv3 system notification entry 75
        Creating an SNMPv3 system notification configuration 76
        Deleting an SNMPv3 system notification configuration 77
    Configuring an SNMPv3 management target address 78
        Creating an SNMPv3 target address configuration 78
        Deleting an SNMPv3 target address configuration 80
    Configuring an SNMPv3 management target parameter 80

Creating an SNMPv3 target parameter configuration 80
Deleting an SNMPv3 target parameter configuration 82
Configuring SNMP traps 82
Creating an SNMP trap receiver configuration 82
Deleting an SNMP trap receiver configuration 83
Configuring EAPOL-based security 84
Managing remote access by IP address 87
Configuring MAC address-based security 89
Configuring MAC address-based security 90
Configuring ports 92
Adding MAC addresses 94
Clearing ports 96
Enabling security on ports 97
Deleting ports 98
Viewing learned MAC addresses by VLAN 99
Locating a specific MAC address 100
Configuring switch port autonegotiation speed 102
Configuring high speed flow control 104
Downloading switch images 105
Storing and retrieving a switch configuration file from a TFTP server 108
Configuring port communication speed 111
Setting system operational modes 112

Chapter 5
Configuring remote network monitoring (RMON). 113

Configuring RMON fault threshold parameters 114
Creating an RMON fault threshold 114
Deleting an RMON threshold configuration 116
Viewing the RMON fault event log 117
Viewing the system log 118
Viewing RMON Ethernet statistics 120
Viewing RMON Ethernet statistics in a bar graph format 122
Viewing RMON Ethernet statistics in a pie chart format 123
Viewing RMON history 124
Viewing RMON statistics in a line graph format 126

Chapter 6
Viewing system statistics 127

Viewing port statistics 127

  Zeroing ports 130

  Viewing port statistics in a pie chart format 131

  Viewing port statistics in a bar graph format 131

Viewing all port errors 132

Viewing interface statistics 134

  Viewing interface statistics in a pie chart format 136

  Viewing interface statistics in a bar graph format 136

Viewing Ethernet error statistics 137

  Viewing Ethernet error statistics in a pie chart format 139

  Viewing Ethernet error statistics in a bar graph format 140

Viewing transparent bridging statistics 141

  Viewing transparent bridging statistics in a pie chart format 143

  Viewing transparent bridging statistics in a bar graph format 144

Chapter 7
Configuring application settings 145

Configuring port mirroring 146

Configuring rate limiting 149

Configuring IGMP 151

Viewing Multicast group membership configurations 153

Creating and managing virtual LANs (VLANs) 155

  Port-based VLANs 156

  Protocol-based VLANs 156

  MAC SA-based VLANs 156

Configuring VLANs 157

  Creating a port-based VLAN 159

  Modifying a port-based VLAN 160

  Creating a protocol-based VLAN 162

  Modifying a protocol-based VLAN 166

  Creating a MAC SA-based VLAN 167

  Modifying a MAC SA-based VLAN 169

  Selecting a management VLAN 171

Deleting a VLAN configuration 172
Configuring broadcast domains 172
Viewing VLAN port information 174
Managing spanning tree groups 176
Creating spanning tree groups 177
Associating STG with VLAN membership 178
Configuring the STG 180
Configuring ports for spanning tree 181
Changing Spanning Tree bridge switch settings 183
Configuring MultiLink Trunk (MLT) members 186
Monitoring MLT traffic 189

Chapter 8
Implementing Quality of Service (QoS) 191

Using QoS Wizard 192
Configuring Standard traffic with the QoS Wizard 192
Prioritizing traffic with the QoS Wizard 194
Prioritizing VLANs with the QoS Wizard 201
Configuring an interface group 204
Creating an interface group configuration 204
Displaying Interface ID Table 207
Adding or removing interface group members 208
Deleting an interface group configuration 210
Configuring 802.1p priority queue assignment 210
Configuring 802.1p priority mapping 212
Creating a DSCP queue assignment 213
Configuring DSCP mapping 215
IP filter and IP filter group configurations 217
Creating an IP filter configuration 218
Deleting an IP filter configuration 222
Creating an IP filter group configuration 222
Modifying an IP filter group configuration 224
Deleting an IP filter group configuration 226
Layer 2 filter and layer 2 filter group configurations 227
Creating a layer 2 filter configuration 227

Deleting a layer 2 filter configuration 232
Creating a layer 2 filter group configuration 233
Modifying a layer 2 filter group configuration 235
Deleting a layer 2 filter group configuration 236
Configuring QoS actions 237
Creating a filter action configuration 237
Creating In-Profile and Out-Profile actions 239
Deleting an action configuration 240
Configuring QoS meters 241
Creating a meter 241
Viewing meters 243
Deleting a meter 243
Configuring QoS policies 244
Installing defined filters 244
Viewing a hardware policy configuration 247
Deleting a hardware policy configuration 248
Configuring QoS Policy Agent (QPA) characteristics 248

Chapter 9
Implementing Common Open Policy Services (COPS). 253

Viewing COPS statistics and capabilities 254
Creating a COPS configuration 257
Deleting a COPS client configuration 260

Chapter 10
Support menu. 261

Using the online help option 261
Downloading technical publications 262
Upgrade option 263
Index 265

Figures

Figure 1 Web-based management interface home page 30
Figure 2 Web page layout 31
Figure 3 Console page 34
Figure 4 System Information home page 38
Figure 5 Console password setting page 40
Figure 6 RADIUS page 41
Figure 7 Web-based management interface log on page 42
Figure 8 System Information home page 43
Figure 9 Reset page 44
Figure 10 Reset to Default page 45
Figure 11 Stack Information page 48
Figure 12 Switch Information page 49
Figure 13 Switch View page 51
Figure 14 Stack Numbering Setting page 54
Figure 15 Identify Unit Numbers page 56
Figure 16 IP page 58
Figure 17 System page 60
Figure 18 SNMPv1 page 62
Figure 19 System Information page 64
Figure 20 User Specification page 66
Figure 21 Group Membership page 69
Figure 22 Group Access Rights page 71
Figure 23 Management Information View page 74
Figure 24 Notification page 76
Figure 25 Target Address page 78
Figure 26 Target Parameter page 81
Figure 27 SNMP Trap Receiver page 83
Figure 28 EAPOL Security Configuration page (1 of 2) 85
Figure 29 EAPOL Security Configuration page (2 of 2) 85

Figure 30 Remote Access page 88
Figure 31 Security Configuration page 90
Figure 32 Port Lists page 92
Figure 33 Port List View, Port List page 93
Figure 34 Port List View, Learn by Ports page 94
Figure 35 Security Table page 95
Figure 36 Port List View, Clear by Ports page 97
Figure 37 Port Configuration page 98
Figure 38 MAC Address Table page 99
Figure 39 Find MAC Address Table page 101
Figure 40 Port Management page 102
Figure 41 High Speed Flow Control page 104
Figure 42 Software Download page 106
Figure 43 Configuration File Download/Upload page 109
Figure 44 Console/Communication Port page 111
Figure 45 Stack Operational Mode page 112
Figure 46 RMON Threshold page 114
Figure 47 RMON Event Log page 117
Figure 48 System Log page 118
Figure 49 RMON Ethernet page 120
Figure 50 RMON Ethernet: Chart in a bar graph format 122
Figure 51 RMON Ethernet: Chart in a pie chart format 123
Figure 52 RMON History page 124
Figure 53 Port page 128
Figure 54 Port: Chart page in a pie chart format 131
Figure 55 Port: Chart page in a bar graph format 132
Figure 56 Port Error Summary page 133
Figure 57 Interface page 134
Figure 58 Interface: Chart in a pie chart format 136
Figure 59 Interface: Chart in a bar graph format 137
Figure 60 Ethernet Errors page 138
Figure 61 Ethernet Error: Chart in a pie chart format 140
Figure 62 Ethernet Error: Chart in a bar graph format 141
Figure 63 Transparent Bridging page 142
Figure 64 Transparent Bridging: Chart in a pie chart format 143

Figure 65 Transparent Bridging: Chart in a bar graph format 144
Figure 66 Port Mirroring page 146
Figure 67 Rate Limiting page 149
Figure 68 IGMP Configuration page 151
Figure 69 IGMP: VLAN Configuration page 152
Figure 70 IGMP Multicast Group Membership page 154
Figure 71 VLAN Configuration page 157
Figure 72 VLAN Configuration: Port Based setting page 159
Figure 73 VLAN Configuration: Port Based modification page 160
Figure 74 VLAN Configuration: Protocol Based setting page 162
Figure 75 VLAN Configuration: Protocol Based modification page 166
Figure 76 VLAN Configuration: MAC SA Based setting page 168
Figure 77 VLAN Configuration: MAC SA Based modification page 169
Figure 78 VLAN Configuration: MAC Address page 170
Figure 79 Port Configuration page 173
Figure 80 Port Information page 175
Figure 81 Spanning Tree Group Creation page 177
Figure 82 Spanning Tree VLAN Membership page 179
Figure 83 Spanning Tree Add VLAN page 179
Figure 84 Spanning Tree Remove VLAN page 180
Figure 85 Spanning Tree Group Setting page 181
Figure 86 Spanning Tree Port Configuration page 182
Figure 87 Spanning Tree Bridge Information page 184
Figure 88 Group page 187
Figure 89 Utilization page 189
Figure 90 QoS Wizard opening page 193
Figure 91 Packet prioritization selection page 193
Figure 92 Standard prioritization page 194
Figure 93 Session confirmation page 194
Figure 94 Packet prioritization explanation page 195
Figure 95 Application prioritization selection page 196
Figure 96 Additional traffic flow prioritization page 196
Figure 97 VLAN prioritization page 197
Figure 98 Session verification page 197
Figure 99 Traffic flow label page 198

Figure 100 Classification rules page 199
Figure 101 Service class assignment page 200
Figure 102 VLAN selection page 202
Figure 103 VLAN service class selection page 202
Figure 104 Interface Configuration page 205
Figure 105 Interface ID page 208
Figure 106 Interface Group Assignment page 209
Figure 107 802.1p Priority Queue Assignment page 211
Figure 108 802.1p Priority Mapping page 213
Figure 109 DSCP Queue Assignment page 214
Figure 110 DSCP Mapping Table page 215
Figure 111 DSCP Mapping Modification page 216
Figure 112 IP Classification page (1 of 3) 218
Figure 113 IP Classification page (2 of 3) 219
Figure 114 IP Classification page (3 of 3) 219
Figure 115 IP Classification Group page 223
Figure 116 IP Group Modification page 225
Figure 117 Layer2 Classification page (1 of 3) 227
Figure 118 Layer2 Classification page (2 of 3) 228
Figure 119 Layer2 Classification page (3 of 3) 228
Figure 120 Layer2 Group page 234
Figure 121 Layer2 Group modification page 235
Figure 122 Action page 238
Figure 123 Meter page 241
Figure 124 Policies page 245
Figure 125 Policy Statistics page 247
Figure 126 Agent page (1 of 2) 249
Figure 127 Agent page (2 of 2) 249
Figure 128 Status page 254
Figure 129 Configuration page 258
Figure 130 Online help window 262
Figure 131 Nortel Networks Technical Documentation Web site 263
Figure 132 Nortel Networks Customer Support Web site 264

Tables

Table 1 Main headings and options 32
Table 2 Menu icons 33
Table 3 Page buttons and icons 35
Table 4 System Information page items 39
Table 5 Console page items 40
Table 6 RADIUS page items 41
Table 7 User levels and access levels 43
Table 8 Stack Information page fields 48
Table 9 Switch Information page fields 50
Table 10 BPS 2000 switch LED descriptions 52
Table 11 Stack Numbering Setting page fields 54
Table 12 IP page items 59
Table 13 System page items 61
Table 14 SNMPv1 page items 63
Table 15 System Information section fields 64
Table 16 SNMPv3 Counters section fields 65
Table 17 User Specification Table section items 66
Table 18 User Specification Creation section items 67
Table 19 Group Membership page items 69
Table 20 Group Access Rights page items 72
Table 21 Management Information View page items 74
Table 22 Notification page items 76
Table 23 Target Address page items 79
Table 24 Target Parameter page items 81
Table 25 SNMP Trap Receiver page items 83
Table 26 EAPOL Security Configuration page fields 86
Table 27 Remote Access page fields 88
Table 28 Security Configuration page items 91
Table 29 Ports Lists page items 93

Table 30 Security Table page items 95
Table 31 Port Configuration page items 98
Table 32 MAC Address Table page items 100
Table 33 Port Management page items 103
Table 34 High Speed Flow Control page items 105
Table 35 Software Download page items 106
Table 36 LED Indications during the software download process 107
Table 37 Configuration File page items 109
Table 38 Requirements for storing or retrieving configuration parameters on a TFTP server 110
Table 39 Parameters not saved to the configuration file 110
Table 40 Console/Communication Port Setting page items 111
Table 41 Stack Operational Mode page items 112
Table 42 RMON Threshold page items 115
Table 43 RMON Event Log page fields 118
Table 44 System Log page fields 119
Table 45 RMON Ethernet page items 120
Table 46 RMON History page items 125
Table 47 Port page items 128
Table 48 Port Error Summary Table fields 133
Table 49 Interface page items 135
Table 50 Ethernet Errors page items 138
Table 51 Transparent Bridging page items 142
Table 52 Port Mirroring page items 147
Table 53 Port-based monitoring modes 148
Table 54 Address-based monitoring modes 148
Table 55 Rate Limiting page items 150
Table 56 IGMP Configuration page items 151
Table 57 IGMP: VLAN Configuration page items 152
Table 58 IGMP Multicast Group Membership page items 154
Table 59 VLAN Configuration page items 158
Table 60 VLAN Configuration: Port Based setting page items 159
Table 61 VLAN Configuration: Port Based modification page items 161
Table 62 VLAN Configuration: Protocol Based setting page items 163
Table 63 Standard protocol-based VLANs and PID types 164

Table 64 Predefined Protocol Identifier (PID) 165
Table 65 VLAN Configuration: Protocol Based modification page items 167
Table 66 VLAN Configuration: MAC SA Based setting page items 168
Table 67 VLAN Configuration: MAC SA Based modification page items 170
Table 68 Port Configuration page items 173
Table 69 Port Information page items 175
Table 70 Spanning Tree Group Creation page items 177
Table 71 Spanning Tree Port Configuration page items 182
Table 72 Spanning Tree Bridge Information page items 184
Table 73 Group page items 188
Table 74 Utilization page items 189
Table 75 Classification rules page items 199
Table 76 QoS Wizard filter limitations 203
Table 77 QoS Interface Queue Table section items 205
Table 78 Interface Group Table section items 206
Table 79 Interface Group Creation section page items 207
Table 80 Interface ID page items 208
Table 81 Interface Group Assignment page items 209
Table 82 802.1p Priority Assignment Table section page items 211
Table 83 802.1p Priority Mapping page items 213
Table 84 DSCP Queue Assignment page items 214
Table 85 DSCP Mapping Table page items 216
Table 86 DSCP Mapping Modification page items 216
Table 87 IP Filter Table and Filter Creation sections page items 220
Table 88 IP Filter Group section page items 223
Table 89 IP Classification Group page items 224
Table 90 IP Modification Group page items 225
Table 91 Layer2 Filter Table and Layer2 Filter Creation section items 228
Table 92 IP Filter Group Table section items 233
Table 93 Layer2 Group page items 234
Table 94 Layer2 Group modification page items 236
Table 95 Action page items 238
Table 96 Meter Creation fields 242
Table 97 Meter Table fields 243
Table 98 Policy page items 246

Table 99 Policy Statistics page items 247
Table 100 Agent page items 250
Table 101 Status page items 254
Table 102 COPS Configuration Table section items 258

Preface

Welcome to *Using Web-based Management for the Business Policy Switch 2000 Software Version 1.2*. This document provides instructions on configuring and managing the Business Policy Switch 2000* through the World Wide Web.

The Web-based management interface is one of many tools specifically designed to assist the network manager in creating complex standalone or network configurations. In addition to the Web-based management system discussed in this book, you can manage the BPS 2000 using SNMP, the Command Line Interface (CLI), Device Manager (DM), or the console interface (CI) menus. Refer to the documents listed "Related publications" on page 22 for information on using and managing the BPS 2000.

This guide describes how to use the Web-based management user interface to configure and maintain your BPS 2000 and the devices connected within its framework.

Before you begin

This guide is intended for network managers who are responsible for configuring BPS 2000es. Consequently, this guide assumes prior knowledge and understanding of the terminology, theories, and practices and specific knowledge about the networking devices, protocols, and interfaces that comprise your network.

You should have working knowledge of the Windows* operating system, graphical user interfaces (GUIs), and Web browsers.

Text conventions

This guide uses the following text conventions:

italic text	Indicates new terms and book titles.
separator (>)	Shows menu paths. Example: Configuration > Port Management identifies the Port Management option on the Configuration menu.

Related publications

For more information about using the Web-based management user interface and the BPS 2000, refer to the following publications:

- *Release Notes for the Business Policy Switch 2000 Software Version 1.2* (part number 210676-D)

  Documents important changes about the software and hardware that are not covered in other related publications.
- *Using the Business Policy Switch 2000 Software Version 1.2* (part number 208700-B)

  Describes how to use the BPS 2000.
- *Business Policy Switch 2000 Installation Instructions* (part number 209319-A*)*

  Describes how to install the BPS 2000.
- *Reference for the Command Line Interface for the Business Policy Switch 2000 Management Software* (part number 212160-A)

  Describes how to use the Command Line Interface (CLI) to configure and manage the BPS 2000.
- *Reference for the Business Policy Switch 2000 Management Software Version 1.2* (part number 209322-B)

Describes how to use the Java Device Manager to configure and manage the BPS 2000.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. (The product family for the BPS 2000 is Data and Internet.) Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1
Using the Web-based management interface

This chapter describes the requirements for using the Web-based management interface and how to use it as a tool to configure your BPS 2000. This chapter covers:

- "New features," next
- "Stacking compatibility" on page 26
- "Software version 1.2 compatibility with BayStack 450 switches" on page 27
- "Requirements" on page 28
- "Port numbering syntax" on page 29
- "Logging in to the Web-based management interface" on page 29
- "Web page layout" on page 30

New features

The following new features that you can access through Web-based management have been introduced to the BPS 2000 software since version 1.0:

- Introduced with software version 1.2
  - VLANS increased to 256
  - Support for multiple spanning tree groups (refer to Chapter 7)
  - IP manager list (refer to Chapter 4)
- Introduced with software version 1.1
  - QoS metering added to policy-enabled networks (refer to Chapter 8)
  - Support for the BayStack 450-1GBIC MDA
  - EAPOL-based security (refer to Chapter 4)
  - Automatic PVID (refer to Chapter 5)

— Table of port statistics (refer to Chapter 6)

Note: To access the software version 1.2 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Stacking compatibility

You can stack the BPS 2000 up to 8 units high. There are two types of stacks:

- Pure BPS 2000—This stack has *only* BPS 2000 switches. It is sometimes referred to as a pure stack. The stack operational mode for this type of stack is Pure BPS 2000 Mode.
- Hybrid—This stack has a combination of BPS 2000 switches *and* BayStack* 450 and/or BayStack 410 switches. It is sometimes referred to as a mixed stack. The stack operational mode for this type of stack is Hybrid Mode.

When you work with the BPS 2000 in standalone mode, you should ensure that the stack operational mode shows Pure BPS 2000 Mode, and does not show Hybrid Mode.

All BPS 2000 switches in the stack must be running the identical version of software, and all the BayStack switches must be running the identical version of software.

When you are working with a mixed stack, you *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for the BayStack 450 switch and BayStack 410 switch must have the same ISVN as the BPS 2000. If the ISVNs are not the same, the stack does not operate.

In sum, the stacking software compatibility requirements are as follows:

- Pure BPS 2000 stack—All units must be running the same software version.

- Pure BayStack 450 stack—All units must be running the same software version.
- Hybrid stack:
  - All BPS 2000 units must be running the same software version.
  - All BayStack 410 units must be running the same software version.
  - All BayStack 450 units must be running the same software version.
  - All software versions must have the identical ISVN.

Refer to Appendix B of *Using the Business Policy Switch 2000 Software Version 1.2* for complete information on interoperability and compatibility between the BPS 2000 and BayStack switches.

Software version 1.2 compatibility with BayStack 450 switches

The BPS 2000 software version 1.2 is compatible with BayStack 450 software version 4.1.

When you are using a local console to access the BPS 2000 software version 1.2 features with a Hybrid, or mixed, stack (BPS 2000 and BayStack 450 and 410 switches in the same stack), you must plug your local console into a BPS 2000 unit.

To find out which version of the BPS 2000 software is running, use the console interface (CI) menus or the Web-based management system:

- CI menus—From the main menu of the console, choose Systems Characteristics menu. The software currently running is displayed in sysDescr.
- Web-based management system—Open the System Information page, which is under Administration on the main menu. The software currently running is displayed in the sysDescription field.

You can use 256 port-, protocol-, and MAC SA-based VLANs for the stack with a Pure BPS 2000 stack running software version 1.2. (The maximum number of MAC SA-based VLANs available is 48). If you are working with a mixed, or Hybrid, stack, you can use 64 VLANs for the entire stack. When you change from a Pure BPS 2000 Stack mode to a Hybrid Stack mode:

- If you have up to 64 VLANs on the Pure BPS 2000 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS 2000 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

Also, a mixed, or Hybrid, stack does not support multiple Spanning Tree Groups (STG). You have a single instance of STG when working with a mixed stack.

- If you have up to 64 VLANs on the Pure BPS 2000 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS 2000 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

Also, a mixed, or Hybrid, stack does not support multiple Spanning Tree Groups (STG). You have a single instance of STG when working with a mixed stack.

Requirements

To use the Web-based management interface, you need the following items:

- A recent computer connected to any of the network ports
- One of the following Web browsers installed on the computer (check the memory requirements):
  - Microsoft Internet Explorer*, version 4.0 or later (Windows 95/98/NT)
  - Netscape Navigator*, version 4.51 or later (Windows 95/98/NT & Unix)
- The IP address of the policy switch
- A web browser optimized for 800 by 600 pixel screen size

Note: The Web-based management interface Web pages may load at different speeds depending on the Web browser you use.

Port numbering syntax

When you enter a port number in a stack configuration, you must specify a unit/port number. A unit/port number consists of the unit number, a slash (/), and the port number. For example, 1/1 is the unit number 1 and port number 1, and 3/11 is unit number 3 and port number 11.

In some cases, you can use a list of ports, or a port list. In this case, the same unit/port number notation applies. In addition, you can use hyphens to specify ranges of ports. For example, 1/1-7,2/1-7,2/9,3/1-4,4/12 is a valid unit/port number list. It represents the following port order:

- Unit 1: ports 1 to 7
- Unit 2: ports 1 to 7 and port 9
- Unit 3: ports 1 to 4
- Unit 4: port 12

Logging in to the Web-based management interface

Before you log in to the Web-based management interface, use the console interface to verify the VLAN port assignments and to ensure that your switch CPU and your computer are assigned to the same VLAN. If the devices are not connected to the same VLAN, you cannot access the Web-based management system.

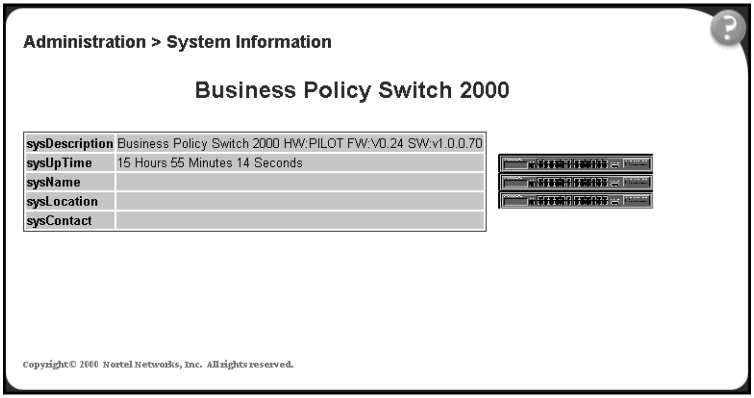
To log in to the Web-based management interface, follow these steps:

1 Start your Web browser.

2 In the Web address field, enter the IP address for your host switch or stack, for example, http://10.30.31.105, and press [Enter].

The home page opens (Figure 1).

Figure 1 Web-based management interface home page



Administration > System Information

Business Policy Switch 2000

sysDescription	Business Policy Switch 2000 HW:PILOT FW:V0.24 SW:v1.0.0.70
sysUpTime	15 Hours 55 Minutes 14 Seconds
sysName	
sysLocation	
sysContact	

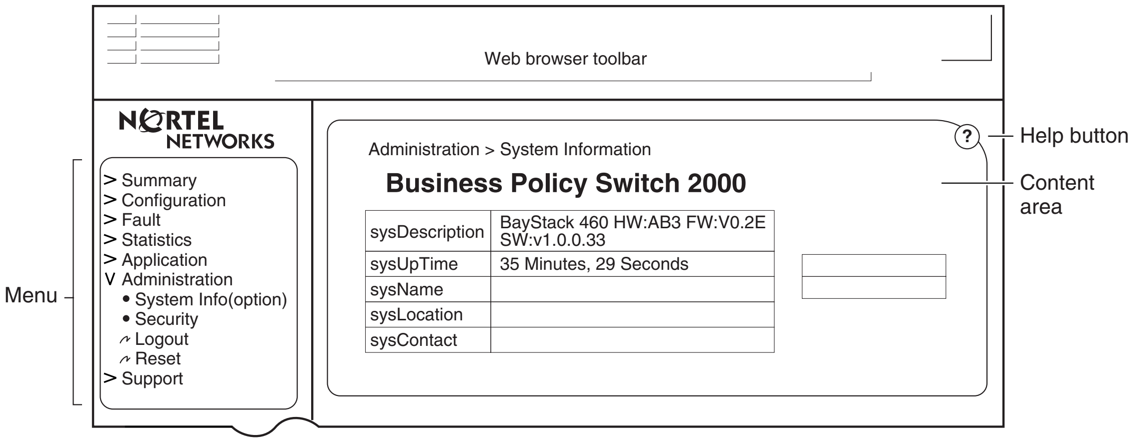
Copyright© 2000 Nortel Networks, Inc. All rights reserved.

Network security does not yet exist the first time you access the Web-based management user interface. As the system administrator, you must create access parameters and passwords to protect the integrity of your network configuration(s). For more information on setting access parameters and system passwords, refer to Chapter 4.

Web page layout

The home Web page (Figure 2) and all successive Web pages have a common layout. Each is divided into two sections: the menu and the management page. All Web pages are optimized for a 800 x 600 pixel screen size.

Figure 2 Web page layout


Web browser toolbar
NORTEL NETWORKS
> Summary
> Configuration
> Fault
> Statistics
> Application
V Administration
• System Info(option)
• Security
Logout
Reset
> Support
Menu
?
Help button
Content area
Administration > System Information
Business Policy Switch 2000

sysDescription	BayStack 460 HW:AB3 FW:V0.2E SW:v1.0.0.33
sysUpTime	35 Minutes, 29 Seconds
sysName	
sysLocation	
sysContact	

9794EA

Menu

The menu, as shown in Figure 2, contains a list of seven main titles and their corresponding options.

To navigate the Web-based management interface menu, click a menu title and then click one of its options. When you click an option, the corresponding page opens.

Table 1 lists the main headings in the Web-based management user interface and their associated options.

Table 1 Main headings and options

Main menu titles	Options
Summary	Stack Information (stack mode only) Switch Information Switch View Identify Unit Numbers (stack mode only) Stack Numbering (stack mode only)
Configuration	IP System Remote Access SNMPv1 SNMPv3* SNMP Trap MAC Address Table Find MAC Address Port Management High Speed Flow Control Software Download Configuration File Console/Comm Port Stack Operational Mode
Fault	RMON Threshold RMON Event Log System Log
Statistics	Port* Port Error Summary Interface* Ethernet Errors* Transparent Bridging* RMON Ethernet* RMON History*
Application	Port Mirroring Rate Limiting EAPOL Security MAC Address Security* IGMP* VLAN* Spanning Tree* Multilink Trunk* QoS* COPS*
Administration	System Information Security* Logout Reset Reset to Defaults
Support	Help Release Notes Manuals Upgrades
*Has additional menus.	

Tools are provided in the menu to assist you in navigating the Web-based management interface.

Caution: Web browser capabilities such as page bookmarking, refresh, and page forward and page back, function as they would in any other Web site. However, these capabilities do not enhance the functionality of the Web-based management interface. Nortel Networks recommends that you use only the navigation tools provided in the management interface.

Table 2 describes the icons that appear on the menu.

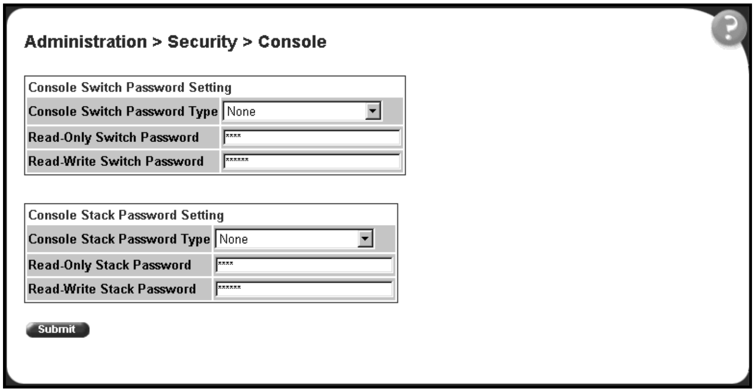
Table 2 Menu icons

Button or icon	Description
➤	This icon identifies a menu title. Click this icon to display its options.
●	This icon identifies a menu title option. Click this icon to display the corresponding page.
◉	This icon identifies a menu title option with a hyperlink to related pages.
↝	This icon is linked an action, for example, logout, reset, or reset to system defaults.
NORTEL NETWORKS	Clicking on the Nortel Networks logo opens the corporate home page in a new Web browser.

Management page

When you click a menu option, the corresponding management page opens. Figure 3 shows the page displayed for the Administration > Security > Console option.

Figure 3 Console page



Administration > Security > Console

Console Switch Password Setting	
Console Switch Password Type	None
Read-Only Switch Password	****
Read-Write Switch Password	******

Console Stack Password Setting	
Console Stack Password Type	None
Read-Only Stack Password	****
Read-Write Stack Password	******

A page is composed of one or more of the following elements:

- Tables and input forms

  The gray cells in a page are display only, and white cells are input fields.

- Check boxes

  You enable or disable a selection by clicking a check box. When a check mark is displayed in the box, that selection is enabled. You disable a selection by clicking the checked box.

- Icons and buttons

  Icons and buttons perform an action concerning the displayed page or the switch. Some pages include a button that opens another page or updates the values shown on the current page. Other pages include icons that initiate an action, such as reformatting the current displayed data as a bar or pie chart.

Table 3 describes the icons that may appear on a pages to assist you in navigation.

Table 3 Page buttons and icons

Icon	Name	Description
📝	Modify	Accesses a modification page for the selected row.
🔍	View	Accesses a view only statistics page for the selected row.
✕	Delete	Deletes a row.
◕	Pie Chart	Displays statistics information in a pie chart format.
📊	Bar Graph	Displays statistics information in a bar graph format.
📈	Line Graph	Displays statistics information in a line graph format.
?	Help	Accesses the Help menu in a new Web browser.
?	Item-Specific Help	Accesses the item-specific Help menu in a new Web browser.
		Note: Text within a table that is highlighted blue and underlined is a hyperlink to a related management page.

Chapter 2
Administering the switch

The administrative options available to you are:

- "Viewing system information," next
- "Configuring system security" on page 39
- "Logging on to the management interface" on page 42
- "Resetting the BPS 2000" on page 43
- "Resetting the BPS 2000 to system defaults" on page 44
- "Logging out of the management interface" on page 45

For more information on the feature discussed in this chapter, refer to *Using the Business Policy Switch 2000 Software Version 1.2*. This book also has instructions using the Console Interface (CI) menus to configure and manage the switch. Refer to *Reference for the Command Line Interface for the Business Policy Switch 2000 Management Software* for instructions on managing the BPS 2000 using the CLI and to *Reference for the Business Policy Switch 2000 Management Software Version 1.2* for instructions on managing the switch using the DM.

➡ **Note:** To access the software version 1.2 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Viewing system information

You can view an image of the BPS 2000 switch or an image of your entire stack configuration, information about the host device (or stack) and, if provided, the contact person or manager for the switch. The System Information page is also the Web-based management interface home page.

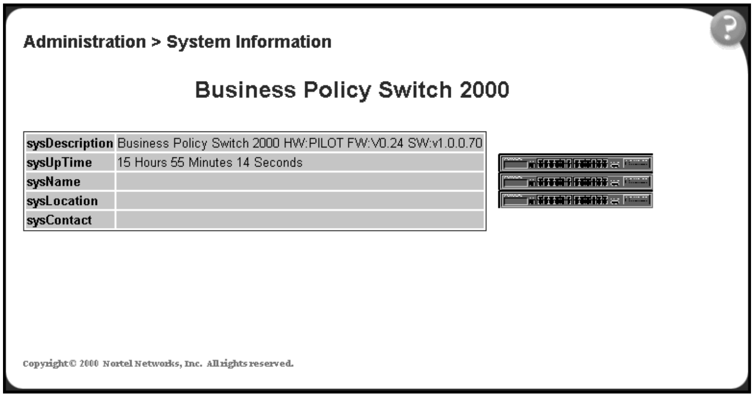
To view system information:

➨ From the main menu, choose Administration > System Information.

The System Information page opens (Figure 4).

Note: You create or modify existing system information parameters on the System page. For more information on configuring system information, refer to Chapter 2.

Figure 4 System Information home page



Administration > System Information

Business Policy Switch 2000

sysDescription	Business Policy Switch 2000 HW:PILOT FW:V0.24 SW:v1.0.0.70
sysUpTime	15 Hours 55 Minutes 14 Seconds
sysName	
sysLocation	
sysContact	

Copyright© 2000 Nortel Networks, Inc. All rights reserved.

Table 4 describes the items on the System Information page.

Table 4 System Information page items

Item	**Description**
sysDescription	The default description of the Business Policy Switch 2000, including the hardware, firmware, software, and ISVN version numbers.
sysUpTime	The elapsed time since the last network management portion of the system was last re-initialized.
sysName	The name created by the network administrator to identify the switch, for example Finance Group.
sysLocation	The location name created by the network administrator to identify the switch location, for example, first floor.
sysContact	The name and email contact information of the administratively assigned person to contact regarding switch operation.

Configuring system security

This section describes the steps you use to build and manage security using the Web-based management interface. For more information on setting security systems, refer to setting EAPOL, MAC security, and IP manager list in Chapter 3.

Setting console, Telnet, and Web passwords

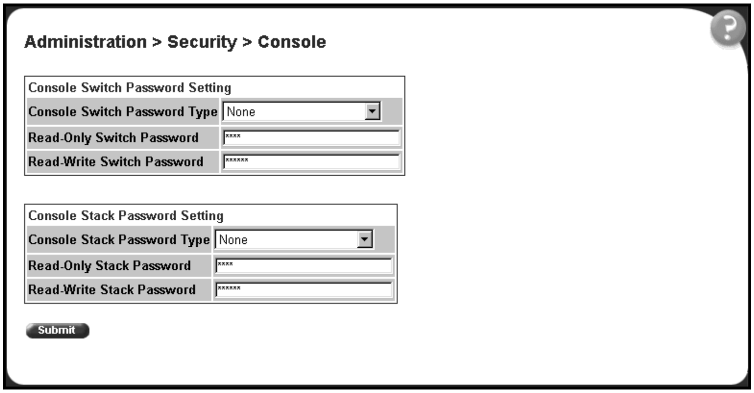
To set console, Telnet, and Web passwords:

1 From the main menu, choose Administration > Security and Console, Telnet, or Web.

The selected password page opens (Figure 5).

➡ **Note:** The title of the page corresponds to the menu selection you choose. In Figure 5, the network administrator selected Administration > Security > Console.

Figure 5 Console password setting page



Administration > Security > Console

Console Switch Password Setting	
Console Switch Password Type	None
Read-Only Switch Password	****
Read-Write Switch Password	******

Console Stack Password Setting	
Console Stack Password Type	None
Read-Only Stack Password	****
Read-Write Stack Password	******

Note: Console, Telnet, and Web settings share the same switch and stack password type and password.

Table 5 describes the items on the Console page.

Table 5 Console page items

Section	Item	Setting	Description
Console Switch Password Setting	Console Switch Password Setting Type	(1) None (2) Local Password (3) RADIUS Authentication	Displays the switch password types. Note: The default is None.
	Read-Only Switch Password	1..15	Type the read-only password setting for the read-only access user.
	Read-Write Switch Password	1..15	Type the read-write password setting for the read-write access user.
Console Stack Password Setting	Console Stack Password Setting Type	(1) None (2) Local Password (3) RADIUS Authentication	Displays the stack password types. Note: The default is None.
	Read-Only Stack Password	1..15	Type the read-only password setting for the read-only access user.
	Read-Write Stack Password	1..15	Type the read-write password setting for the read-write access user.

2 Type the information, or make a selection from the list.

3 Click Submit.

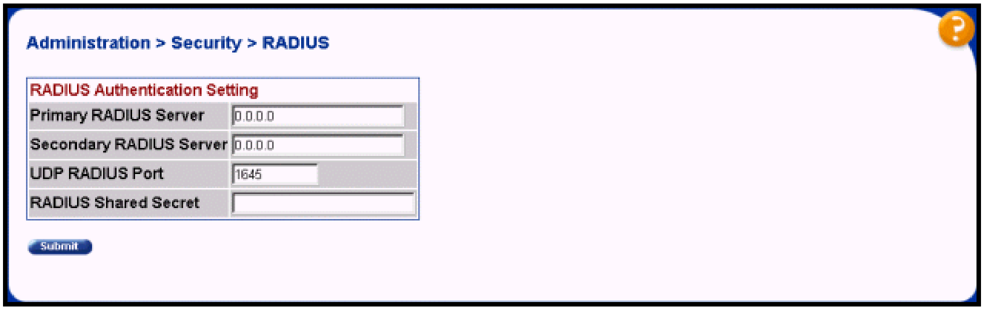
Configuring RADIUS security

To configure RADIUS security parameters:

1 From the main menu, choose Administration > Security > RADIUS.

The RADIUS page opens.

Figure 6 RADIUS page



Administration > Security > RADIUS

RADIUS Authentication Setting

Primary RADIUS Server	0.0.0.0
Secondary RADIUS Server	0.0.0.0
UDP RADIUS Port	1645
RADIUS Shared Secret	

Table 6 describes the items on the RADIUS page.

Table 6 RADIUS page items

Item	Setting	Description
Primary RADIUS Server	XXX.XXX.XXX.XXX	Type a Primary RADIUS server IP address in the appropriate format.
Secondary RADIUS Server	XXX.XXX.XXX.XXX	Type a Secondary RADIUS server IP address in the appropriate format.
UDP RADIUS Port	Integer	Type the UDP RADIUS port number.
RADIUS Shared Secret	1..16	Type a unique character string to create a secret password.

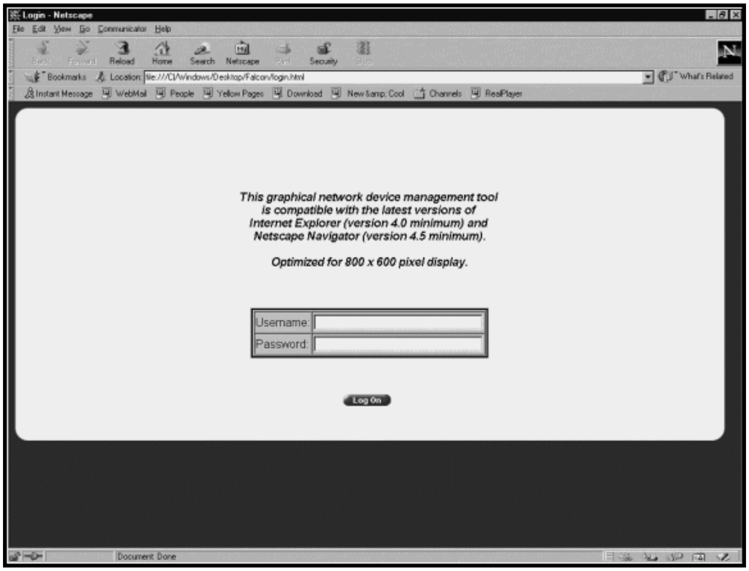
2 Type the information.

3 Click Submit.

Logging on to the management interface

Once switch and stack passwords and RADIUS authentication settings are integrated into the Web-based management user interface, anyone who attempts to use the application is presented with a log on page (Figure 7).

Figure 7 Web-based management interface log on page



Login - Netscape
File Edit View Go Communicator Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Stop
Bookmarks
Location: file:///C|/Windows/Desktop/Falcon/login.html
What's Related
Instant Message
WebMail
People
Yellow Pages
Download
New&amp; Cool
Channels
RealPlayer
Username:
Password:
Log On
Document: Done

This graphical network device management tool is compatible with the latest versions of Internet Explorer (version 4.0 minimum) and Netscape Navigator (version 4.5 minimum).

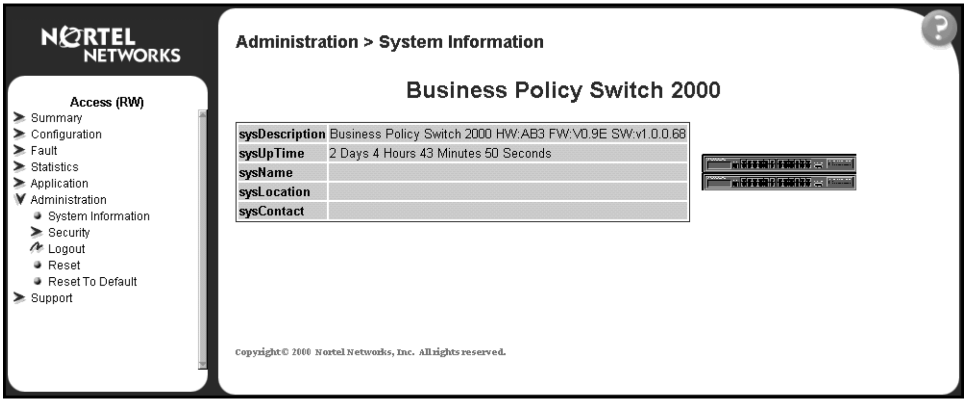
Optimized for 800 x 600 pixel display.

To log on to the Web-based management interface:

1. In the Username text box, type **`RO`** for read-only access or **`RW`** for read-write access.
2. In the Password text box, type your password.
3. Click Log On.

   The System Information home page opens (Figure 8).

Figure 8 System Information home page


NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Administration
System Information
Security
Logout
Reset
Reset To Default
Support
?

Administration > System Information

Business Policy Switch 2000

sysDescription	Business Policy Switch 2000 HW:AB3 FW:V0.9E SW:v1.0.0.68
sysUpTime	2 Days 4 Hours 43 Minutes 50 Seconds
sysName	
sysLocation	
sysContact	

Copyright© 2000 Nortel Networks, Inc. All rights reserved.

With Web access enabled, the switch can support up to four concurrent Web page users. Two predefined user levels are available, and each user level has a corresponding username and password.

Table 7 shows an example of the two predefined user levels available and their access level within the Web-based management user interface.

Table 7 User levels and access levels

User level	User name for each level	Password for each user level	Access Level
Read-only	RO	XXXXXXXX	Read only
Read-write	RW	XXXXXXXX	Full read/write access

Resetting the BPS 2000

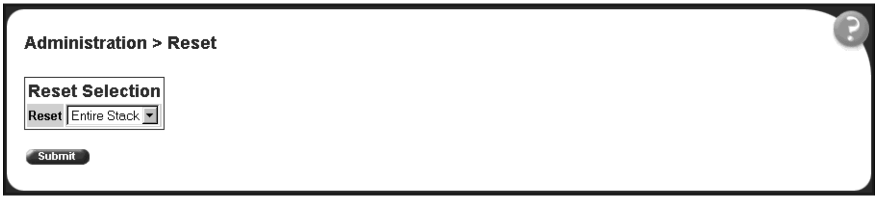
You can reset a standalone switch, a specific unit in a stack configuration, or an entire stack without erasing any configured switch parameters. While resetting, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress. (Resetting means rebooting in this context.)

To reset the BPS 2000 without making changes (since your last Submit request):

1 From the main menu, choose Administration > Reset.

The Reset page opens (Figure 9).

Figure 9 Reset page



2 From the list, choose to reset the switch only, or the entire stack.

3 Click Submit.

Note: If you have not configured system password security, a reset returns you to the home page, as shown in Figure 1 on page 30. If you have configured system password security, a reset returns you to a log on page, as shown in Figure 7 on page 42.

Resetting the BPS 2000 to system defaults

You can reset a standalone switch, a specific unit in a stack configuration, or an entire stack, replacing all configured switch parameters with the factory default values.

Caution: If you choose reset to default settings, all configured settings are replaced with factory default settings when you click Submit (Stack Operational Mode is not reset to factory default}. For more information on factory default settings, see *Using the Business Policy Switch 2000* (208700-A).

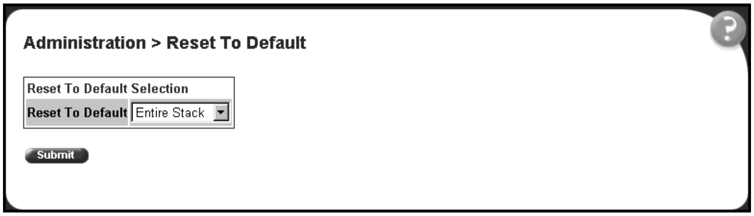
During the reset process, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

To reset the BPS 2000 to system defaults:

1 From the main menu, choose Administration > Reset to Default.

The Reset to Default page opens (Figure 10).

Figure 10 Reset to Default page



Administration > Reset To Default

Reset To Default Selection	
Reset To Default	Entire Stack

2 From the list, choose to reset the switch only to system defaults, or the entire stack.

3 Click Submit.

Note: If you have not configured system password security, a reset returns you to the home page, as shown in Figure 1 on page 30. If you have configured system password security, a reset returns you to a log on page, as shown in Figure 7 on page 42.

Logging out of the management interface

To log out of the Web-based management interface:

1 From the main menu, choose Administration > Logout.

A message opens prompting you to confirm your request

2 Do one of the following:

- Click OK to logout of the Web-based management interface.
- Click Cancel to return to the Web-based management interface home page.

Chapter 3
Viewing summary information

The summary information options are:

- "Viewing stack information," next
- "Viewing summary switch information" on page 49
- "Viewing switch information in real time" on page 51
- "Changing stack numbering" on page 54
- "Identifying unit numbers" on page 56

→ **Note:** To access the software version 1.2 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Viewing stack information

You can view a summary of your stack framework, for example, the current version of the running software and the IP address of the Web-based management interface.

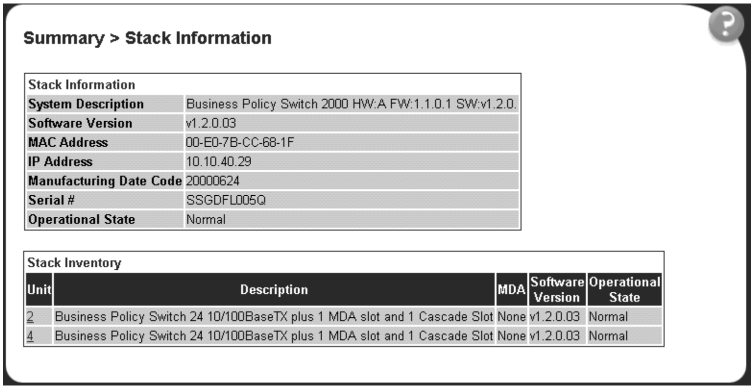
→ **Note:** The Web-based management user interface automatically detects the operational mode of your system. If the system is in standalone mode, the Stack Information page is not an option listed in the menu. For information on how to set system operational modes, see "Setting system operational modes" on page 112.

To view stack information:

1. From the main menu, choose Summary > Stack Information.

   The Stack Information page opens (Figure 11).

Figure 11 Stack Information page



Summary > Stack Information

Stack Information	
System Description	Business Policy Switch 2000 HW:A FW:1.1.0.1 SW:v1.2.0.
Software Version	v1.2.0.03
MAC Address	00-E0-7B-CC-68-1F
IP Address	10.10.40.29
Manufacturing Date Code	20000624
Serial #	SSGDFL005Q
Operational State	Normal

Stack Inventory

Unit	Description	MDA	Software Version	Operational State
2	Business Policy Switch 24 10/100BaseTX plus 1 MDA slot and 1 Cascade Slot	None	v1.2.0.03	Normal
4	Business Policy Switch 24 10/100BaseTX plus 1 MDA slot and 1 Cascade Slot	None	v1.2.0.03	Normal

Table 8 describes the fields on the Stack Information and Stack Inventory sections of the Stack Information page.

Table 8 Stack Information page fields

Section	Fields	Description
Stack Information	System Description	The name created in the configuration process to identify the stack.
	Software Version	The version of the running software.
	MAC Address	The MAC address of the stack.
	IP Address	The IP address of the stack.
	Manufacturing Date Code	The date of manufacture of the board in ASCII format: YYYYMMDD.
	Serial Number	The serial number of the base unit.
	Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured
Stack Inventory	Unit	The unit number assigned to the device by the network manager. For more information on stack numbering, see page 54.
	Description	The description of the device or its subcomponent.
	MDA	The media dependent adapter (MDA) connected to the switch.

Table 8 Stack Information page fields (continued)

Section	Fields	Description
	Software Version	The current running software version.
	Operational State	The current operational state of the stack. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.

2 In the upper-left corner of the Stack Information page, click the number of the device you want to view.

The Stack Information page is updated with information about the selected switch.

Viewing summary switch information

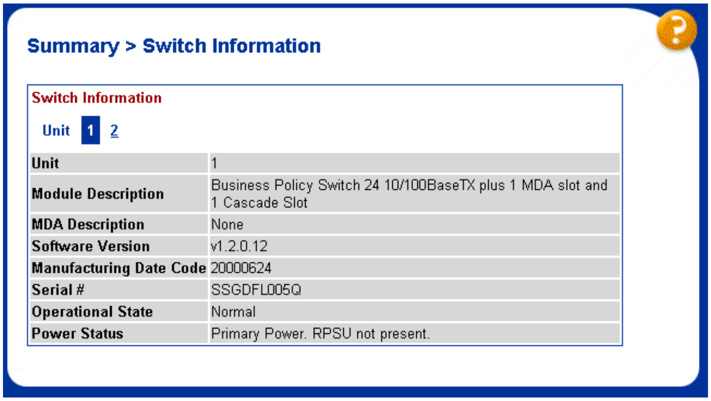
You can view summary information about the switch, for example, the unit number and its corresponding physical description and serial number.

To view summary switch information:

1 From the main menu, choose Summary > Switch Information.

The Switch Information page opens (Figure 12).

Figure 12 Switch Information page



Unit	1
Module Description	Business Policy Switch 24 10/100BaseTX plus 1 MDA slot and 1 Cascade Slot
MDA Description	None
Software Version	v1.2.0.12
Manufacturing Date Code	20000624
Serial #	SSGDFL005Q
Operational State	Normal
Power Status	Primary Power. RPSU not present.

Table 9 describes the fields on the Switch Information page.

Table 9 Switch Information page fields

Item	Description
Unit	Select the number of the device on which to view summary information. The page is updated with information about the selected switch. For more information on stack numbering, see page 54.
Module Description	The factory set description of the policy switch.
MDA Description	The factory set description of the sub-component/MDA.
Software Version	The version of the running software.
Manufacturing Date Code	The date of manufacture of the board in ASCII format.
Serial Number	The serial number of the policy switch.
Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.
Mac Address	The MAC address of the device.
IP Address	The IP address of the device.
Power Status	The current power status of the device: • Primary Power. RPSU not present • Primary Power. RPSU present • Redundant Power. Primary power failed • Unavailable

2 In the upper-left corner of the Switch Information page, click the number of the device you want to view.

The Switch Information page is updated with information about the selected switch.

Viewing switch information in real time

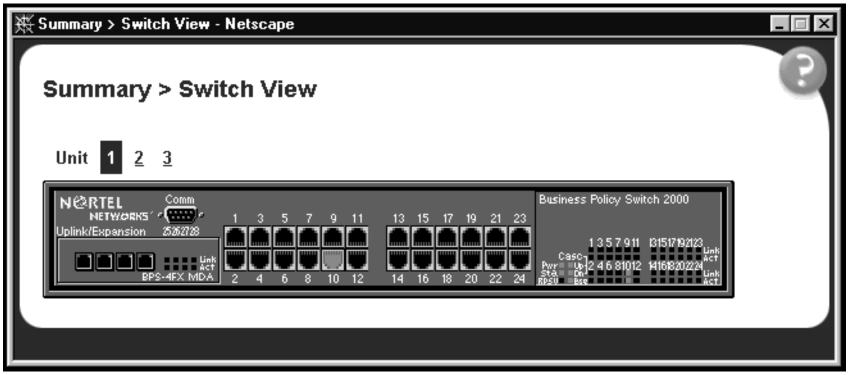
You can display the port and LED status information of a selected policy switch in real time.

To display a physical view of the policy switch:

1 From the main menu, choose Summary > Switch View.

The Switch View page opens in a separate Web browser (Figure 13).

Figure 13 Switch View page


Summary > Switch View - Netscape
Summary > Switch View
Unit 1 2 3
NORTEL NETWORKS
Comm
Uplink/Expansion
25 26 27 28
BPS-4FX MDA
Link
Act
1 3 5 7 9 11
2 4 6 8 10 12
13 15 17 19 21 23
14 16 18 20 22 24
Business Policy Switch 2000
Casc
Pwr
Sta
RPSU
Up
Dn
Bse

Note: You may be presented with a security warning to click on before the switch view appears.

Table 10 describes the fields on the Switch View page.

Table 10 BPS 2000 switch LED descriptions

Label	Type	Color	State	Meaning
Pwr	Power status	Green	On	DC power is available to the switch’s internal circuitry.
			Off	No AC power to switch or power supply failed.
Status	System status	Green	On	Self-test passed successfully and switch is operational.
			Blinking	A nonfatal error occurred during the self-test.
			Off	The switch failed the self-test.
RPSU	RPSU status	Green	On	The switch is connected to the RPSU and can receive power if needed.
			Off	The switch is not connected to the RPSU or RPSU is not supplying power.
CAS Up Stack mode			Off	The switch is in standalone mode.
		Green	On	The switch is connected to the *upstream* unit’s Cascade A In connector.
		Amber	On	The Cascade A Out connector (CAS Up) for this switch is looped internally (wrapped to the secondary ring).
CAS Dwn Stack mode			Off	The switch is in standalone mode.
		Green	On	The switch is connected to the *downstream* unit’s Cascade A Out connector.
		Amber	On	The Cascade A In connector (CAS Dwn) for this switch is looped internally (wrapped to the secondary ring).

Table 10 BPS 2000 switch LED descriptions (continued)

Label	Type	Color	State	Meaning
Base	Base mode	Green	On	The switch is configured as the stack base unit.
			Off	The switch is *not* configured as the stack base unit (or is in standalone mode).
		Amber	On	This unit is operating as the stack configuration's *temporary base unit*. This condition occurs automatically if the base unit (directly downstream from this unit) fails. If this happens, the following events take place: The two units directly upstream and directly downstream from the failed unit automatically wrap their cascade connectors and indicate this condition by lighting their Cas Up and Cas Dwn LEDs (see Cas Up and Cas Dwn description in this table). If the temporary base unit fails, the next unit directly downstream from this unit becomes the new temporary base unit. This process can continue until there are only two units left in the stack configuration. This automatic failover is a temporary safeguard only. If the stack configuration loses power, the temporary base unit will not power up as the base unit when power is restored. For this reason, you should always assign the temporary base unit as the base unit (set the Unit Select switch to Base) until the failed unit is repaired or replaced.
10/100	10/100 Mb/s port speed indicator	Green	On	The corresponding port is set to operate at 100 Mb/s and the link is good.
		Amber	On	The corresponding port is set to operate at 10 Mb/s and the link is good.
			Off	The link connection is bad or there is no connection to this port.
Link	Link status	Green	On	Valid communications link established.
			Off	The communications link connection is bad or there is no connection to this port.
Activity	Port activity	Green or Amber	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

2 In the upper-left corner of the Switch View page, click the number of the device you want to view.

The Switch View page is updated with a view of the selected switch.

Changing stack numbering

If your system is set to “stack” operational mode, you can view existing stack numbering information and renumber the devices in your stack framework. For information on how to set your system’s operational mode, see “Setting system operational modes” on page 112.

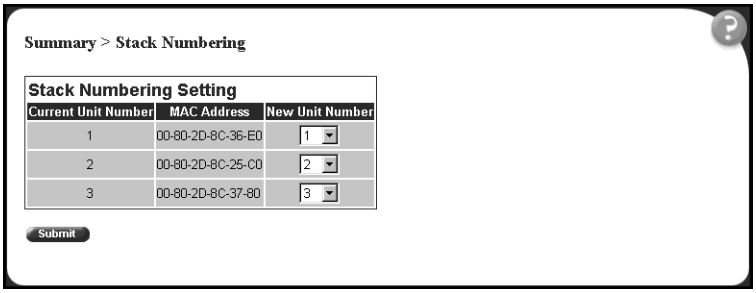
Note: The unit number does not affect the base unit designation.

To view or renumber devices within the stack framework:

1 From the main menu, choose Summary > Stack Numbering.

The Stack Numbering Setting page opens (Figure 14).

Figure 14 Stack Numbering Setting page



Stack Numbering Setting

Current Unit Number	MAC Address	New Unit Number
1	00-80-2D-8C-36-E0	1
2	00-80-2D-8C-25-C0	2
3	00-80-2D-8C-37-80	3

Table 11 describes the fields on the Stack Numbering Setting page.

Table 11 Stack Numbering Setting page fields

Item	Range	Description
Current Unit Number	1..8	Unit number previously assigned to the policy switch. The entries in this column are displayed in order of their current physical cabling with respect to the base unit, and can show nonconsecutive unit numbering if one or more units were previously moved or modified. The entries can also include unit numbers of units that are no longer participating in the stack (not currently active).

Table 11 Stack Numbering Setting page fields (continued)

Item	Range	Description
MAC Address	XX.XX.XX.XX.XX.XX	MAC address of the corresponding unit listed in the Current Unit Number field.
New Unit Number	1..8, None	Choose a new number to assign to your selected policy switch. Note: If you leave the field blank, the system automatically selects the next available number.

2 Choose the new number to assign to your switch.

3 Click Submit.

A message opens prompting you to confirm your request.

4 Do one of the following:

- Click OK to renumber the stack.
- Click Cancel to return to the Stack Numbering page without making changes.

Identifying unit numbers

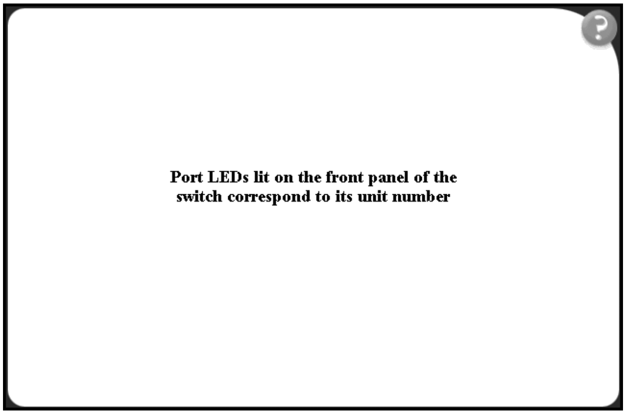
You can identify the unit numbers of the switches participating in a stack configuration by viewing the LEDs on the front panel of each switch.

To identify unit numbers in your configuration:

1. From the main menu, choose Summary > Identify Unit Numbers.

   The Identify Unit Numbers page opens (Figure 15).

Figure 15 Identify Unit Numbers page



Port LEDs lit on the front panel of the switch correspond to its unit number

2. To continue viewing summary information or to start the configuration process, choose another option from the main menu.

Chapter 4

Configuring the switch

The switch configuration options available to you are:

- "Configuring BootP, IP, and gateway settings," (next)
- "Modifying system settings" on page 60
- "About SNMP" on page 61
- "Configuring SNMPv1" on page 62
- "Configuring SNMPv3" on page 63
- "Configuring SNMP traps" on page 82
- "Configuring EAPOL-based security" on page 84
- "Managing remote access by IP address" on page 87
- "Configuring MAC address-based security" on page 89
- "Viewing learned MAC addresses by VLAN" on page 99
- "Locating a specific MAC address" on page 100
- "Configuring switch port autonegotiation speed" on page 102
- "Configuring high speed flow control" on page 104
- "Downloading switch images" on page 105
- "Storing and retrieving a switch configuration file from a TFTP server" on page 108
- "Configuring port communication speed" on page 111
- "Setting system operational modes" on page 112

➡ **Note:** To access the software version 1.2 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Configuring BootP, IP, and gateway settings

You can configure your BootP mode settings, create and modify your in-band stack and in-band switch IP addresses and in-band subnet mask parameters, and configure the IP address of your default gateway.

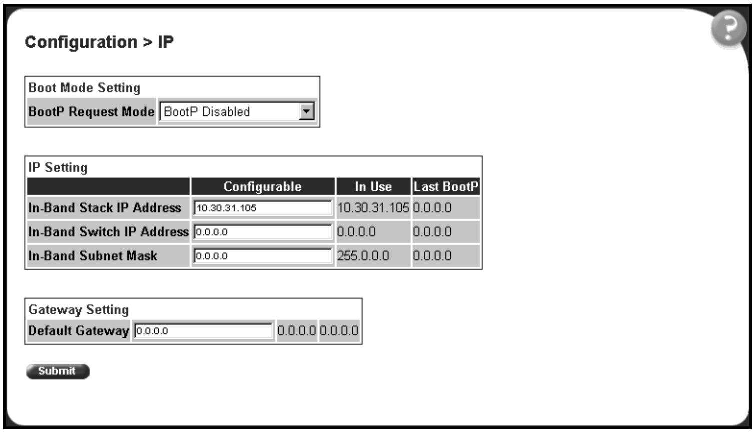
Note: Settings take effect immediately when you click Submit.

To configure BootP, IP, and gateway settings:

1 From the main menu, choose Configuration > IP.

The IP page opens (Figure 16).

Figure 16 IP page



Configuration > IP

Boot Mode Setting

BootP Request Mode	BootP Disabled

IP Setting

	Configurable	In Use	Last BootP
In-Band Stack IP Address	10.30.31.105	10.30.31.105	0.0.0.0
In-Band Switch IP Address	0.0.0.0	0.0.0.0	0.0.0.0
In-Band Subnet Mask	0.0.0.0	255.0.0.0	0.0.0.0

Gateway Setting

Default Gateway	0.0.0.0	0.0.0.0	0.0.0.0

Table 12 describes the items on the IP page.

Table 12 IP page items

Section	Item	Range	Description
Boot Mode Setting	BootP Request Mode	BootP When Needed	Choose this mode to inform the switch to send a BootP request when the switch IP address stored in nonvolatile memory is the factory default value. If the stored IP address differs from the factory default value, the switch uses the stored network parameters. If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings
		BootP Always	Choose this mode to inform the switch, each time the switch boots, to ignore any stored network parameters and send a BootP request. If the BootP request fails, the switch boots with the factory default IP configuration. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to boot normally.
		BootP Disabled	Choose this mode to inform the switch, each time the switch boots, to use the IP configuration parameters stored in non-volatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops.
		BootP or Last Address	Choose this mode to inform the switch, at each startup, to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its non-volatile memory. Note: Valid parameters obtained in using BootP always replace current information stored in the non-volatile memory.
		Note: Whenever the switch is broadcasting BootP requests, the BootP process times out if a reply is not received within (approximately) 7 minutes. When the process times out, the BootP request mode automatically changes to BootP Disabled mode. To restart the BootP process, change the BootP request mode to any of the three following modes: BootP When Needed, BootP Always, or to BootP or Last Address.	
IP Setting	In-Band Stack IP Address	XXX.XXX.XXX.XXX	Type a new stack IP address in the appropriate format.
	In-Band Switch IP Address	XXX.XXX.XXX.XXX	Type a new switch IP address in the appropriate format. Note: When the IP address is entered in the In-Band IP Address field, and the In-Band Subnet Mask field value is not present, the software provides an *in-use* default value for the In-Band Subnet Mask field that is based on the class of the IP address entered in the In-Band IP Address field.
	In-Band Subnet Mast	XXX.XXX.XXX.XXX	Type a new subnet mask in the appropriate format.
	In-Use		The column header for the read-only fields in this screen. The data displayed in this column represents data that is currently in use.
	Last BootP		The column header for the read-only fields in this screen. The read-only data displayed in this column represents data obtained from the last BootP reply received.
Gateway Setting	Default Gateway	XXX.XXX.XXX.XXX	Type an IP address for the default gateway in the appropriate format.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Modifying system settings

You can create or modify the system name, system location, and network manager contact information.

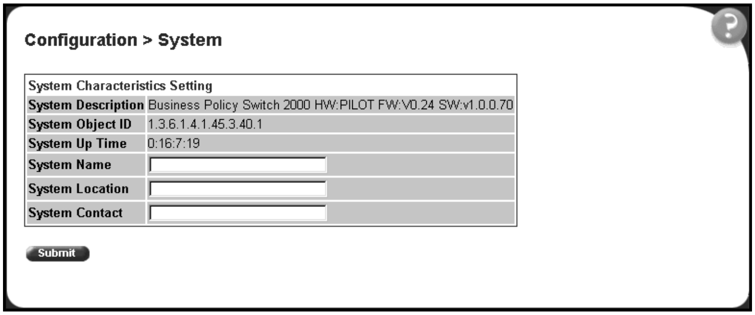
Note: The configurable parameters on the System page are displayed in a read only-format on the Web-based management user interface System Information home page (see Figure 1 on page 30).

To configure system settings:

1 From the main menu, choose Configuration > System.

The System page opens (Figure 17).

Figure 17 System page



Configuration > System

System Characteristics Setting	
System Description	Business Policy Switch 2000 HW:PILOT FW:V0.24 SW:v1.0.0.70
System Object ID	1.3.6.1.4.1.45.3.40.1
System Up Time	0:16:7:19
System Name	
System Location	
System Contact	

Table 13 describes the items on the System page.

Table 13 System page items

Item	Range	Description
System Description		The factory set description of the hardware and software versions.
System Object ID		The character string that the vendor created to uniquely identify this device.
System Up Time		The elapsed time since the last network management portion of the system was last re-initialized. Note: This field is updated only when the screen is redisplayed.
System Name	0..255	Type a character string to create a name to identify the switch, for example Finance Group.
System Location	0..255	Type a character string to create a name for the switch location, for example, First Floor.
System Contact	0..255	Type a character string to create the contact information for the network manager or the selected person to contact regarding switch operation, for example, mcarlson@company.com Note: To operate correctly with the Web interface, the system contact should be an e-mail address.

2. Type information in the text boxes.
3. Click Submit.

About SNMP

Simple Network Management Protocol (SNMP) is the standard for network management that uses a common software agent to manage local and wide area network equipment from different vendors; part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and defined in RFC1157. SNMPv1 is version one, or the original standard protocol. SNMPv3 is a combination of proposal updates to SNMP, most of which deal with security.

Configuring SNMPv1

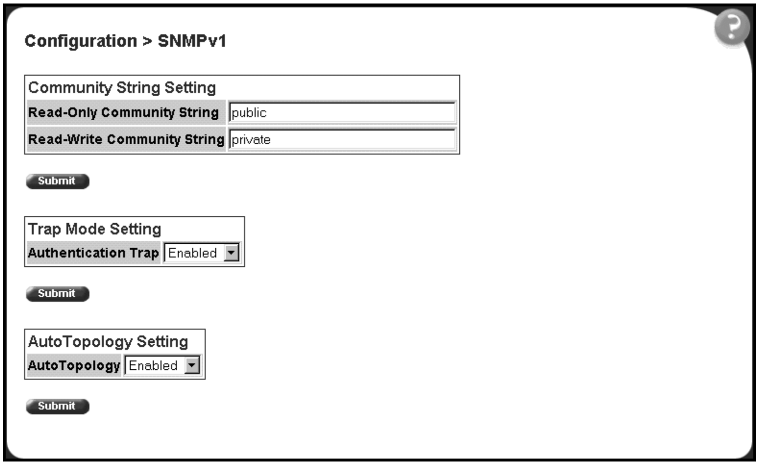
You can configure SNMPv1 read-write and read-only community strings, enable or disable trap mode settings, and/or enable or disable the Autotopology feature. The Autotopology feature, when enabled, performs a process that recognizes any device on the managed network and defines and maps its relation to other network devices in real time.

To configure the community string, trap mode, and Autotopology settings and features:

1. From the main menu, choose Configuration > SNMPv1.

   The SNMPv1 page opens (Figure 18).

Figure 18 SNMPv1 page



Configuration > SNMPv1

Community String Setting

Read-Only Community String	public
Read-Write Community String	private

Trap Mode Setting

Authentication Trap	Enabled

AutoTopology Setting

AutoTopology	Enabled

Table 14 describes the items on the SNMPv1 page.

Table 14 SNMPv1 page items

Section	Item	Range	Description
Community String Setting	Read-Only Community String	1..32	Type a character string to identify the community string for the SNMPv1 read-only community, for example, public or private. The default value is public.
	Read-Write Community String	1..32	Type a character string to identify the community string for the SNMPv1 read-write community, for example, public or private. The default value is private.
Trap Mode Setting	Authentication Trap	(1) Enable (2) Disable	Choose to enable or disable the authentication trap.
AutoTopology Setting	AutoTopology	(1) Enable (2) Disable	Choose to enable or disable the autotopology feature.

2 Type information in the text boxes, or select from a list.

3 Click Submit in any section to save your changes.

Configuring SNMPv3

This section describes the steps to build and manage SNMPv3 in the Web-based management user interface.

Viewing SNMPv3 system information

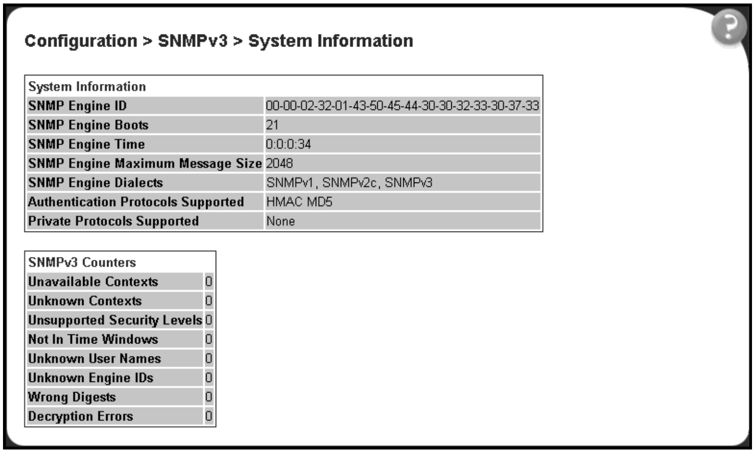
You can view information about the SNMPv3 engine that exists and the private protocols that are supported in your network configuration. You can also view information about packets received by the system having particular errors, such as unavailable contexts, unknown contexts, decrypting errors, or unknown user names.

To view SNMPv3 system information:

1 From the main menu, choose Configuration > SNMPv3 > System Information.

The System Information page opens (Figure 19).

Figure 19 System Information page



Configuration > SNMPv3 > System Information

System Information	
SNMP Engine ID	00-00-02-32-01-43-50-45-44-30-30-32-33-30-37-33
SNMP Engine Boots	21
SNMP Engine Time	0:0:0:34
SNMP Engine Maximum Message Size	2048
SNMP Engine Dialects	SNMPv1 , SNMPv2c , SNMPv3
Authentication Protocols Supported	HMAC MD5
Private Protocols Supported	None

SNMPv3 Counters	
Unavailable Contexts	0
Unknown Contexts	0
Unsupported Security Levels	0
Not In Time Windows	0
Unknown User Names	0
Unknown Engine IDs	0
Wrong Digests	0
Decryption Errors	0

Table 15 describes the fields on the System Information section of the SNMPv3 System Information page.

Table 15 System Information section fields

Item	**Description**
SNMP Engine ID	The SNMP engine's identification number.
SNMP Engine Boots	The number of times that the SNMP engine has re-initialized itself since its initial configuration.
SNMP Engine Time	The number of seconds since the SNMP engine last incremented the snmpEngineBoots object.
SNMP Engine Maximum Message Size	The maximum length, in octets, of an SNMP message which this SNMP engine can send or receive and process determined as the minimum of the maximum message size values supported among all transports available to and supported by the engine.
SNMP Engine Dialects	The SNMP dialect the engine recognizes. The dialects are:SNMP1v1, SNMPv2C, and SNMPv3.
Authentication Protocols Supported	The registration point for standards-track authentication protocols used in SNMP Management Frameworks. The registration points are: None, HMAC MD5. Note: The Business Policy Switch 2000 supports only the MD5 authentication protocol.
Private Protocols Supported	The registration point for standards-track privacy protocols used in SNMP Management Frameworks. The registration points are: None or CBC-DES. Note: The Business Policy Switch 2000 does not support privacy protocols.

Table 16 describes the fields on the SNMPv3 Counters section of the SNMPv3 System Information page.

Table 16 SNMPv3 Counters section fields

Item	Description
Unavailable Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unavailable.
Unknown Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unknown.
Unsupported Security Levels	The total number of packets dropped by the SNMP engine because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
Not in Time Windows	The total number of packets dropped by the SNMP engine because they appeared outside of the authoritative SNMP engine's window.
Unknown User Names	The total number of packets dropped by the SNMP engine because they referenced an unknown user.
Unknown Engine IDs	The total number of packets dropped by the SNMP engine because they referenced an snmpEngineID that was not known to the SNMP engine.
Wrong Digests	The total number of packets dropped by the SNMP engine because they did not contain the expected digest value.
Decryption Errors	The total number of packets dropped by the SNMP engine because they could not be decrypted.

Configuring user access to SNMPv3

You can view a table of all current SNMPv3 user security information such as authentication/privacy protocols in use, and create or delete SNMPv3 system user configurations.

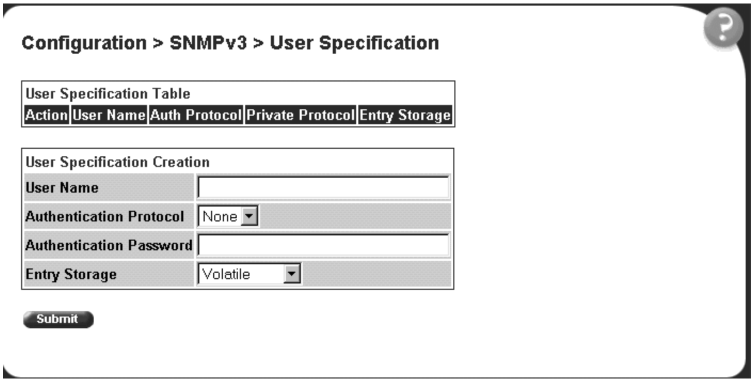
Creating an SNMPv3 system user configuration

To create an SNMPv3 system user configuration:

1 From the main menu choose Configuration > SNMPv3 > User Specification.

The User Specification page opens (Figure 20).

Figure 20 User Specification page



Configuration > SNMPv3 > User Specification

User Specification Table

Action	User Name	Auth Protocol	Private Protocol	Entry Storage

User Specification Creation

User Name	
Authentication Protocol	None
Authentication Password	
Entry Storage	Volatile

Table 17 describes the items on the User Specification Table section of the User Specification page.

Table 17 User Specification Table section items

Item and MIB association	Description
☒	Deletes the row.
User Name (usmUserSecurityName)	The name of an existing SNMPv3 user.
Authentication Protocol (usmUserAuthProtocol)	Indicates whether the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated by the MD5 authentication protocol. Note: The Business Policy Switch 2000 supports only the MD5 authentication protocol.
Private Protocol (usmUserPrivProtocol)	Displays whether or not messages sent on behalf of this user to or from the SNMP engine identified by usmUserEngineID can be protected from disclosure, and if so, the type of privacy protocol which is used.
Entry Storage	The current storage type for this row. If “Volatile” is displayed, information is dropped (lost) when you turn the power off. If non-volatile is displayed, information is saved in NVRAM when you turn the power off

Table 18 describes the items on the User Specification Creation section of the User Specification page.

Table 18 User Specification Creation section items

Item and MIB association	Range	Description
User Name	1..32	Type a string of characters to create an identity for the user.
Authentication Protocol (usmUserAuthProtocol)	None MD5	Choose whether or not the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated with the MD5 protocol. Note: The Business Policy Switch 2000 supports only the MD5 authentication protocol.
Authentication Password (usmUserAuthPassword)	1..32	Type a string of character to create a password to use in conjunction with the authorization protocol.
Entry Storage (usmUserStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2. In the User Specification Creation section, type information in the text boxes, or select from a list.
3. Click Submit.

   The new configuration is displayed in the User Specification Table (Figure 20).

Deleting an SNMPv3 system user configuration

To delete an existing SNMPv3 user configuration:

1. From the main menu, choose Configuration > SNMPv3 > User Specification.

   The User Specification page opens (Figure 20).

2. In the User Specification Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the SNMPv3 user configuration.
   - Click Cancel to return to the User Specification page without making changes.

Configuring an SNMPv3 system user group membership

You can view a table of existing SNMPv3 group membership configurations and map or delete an SNMPv3 user to group configuration.

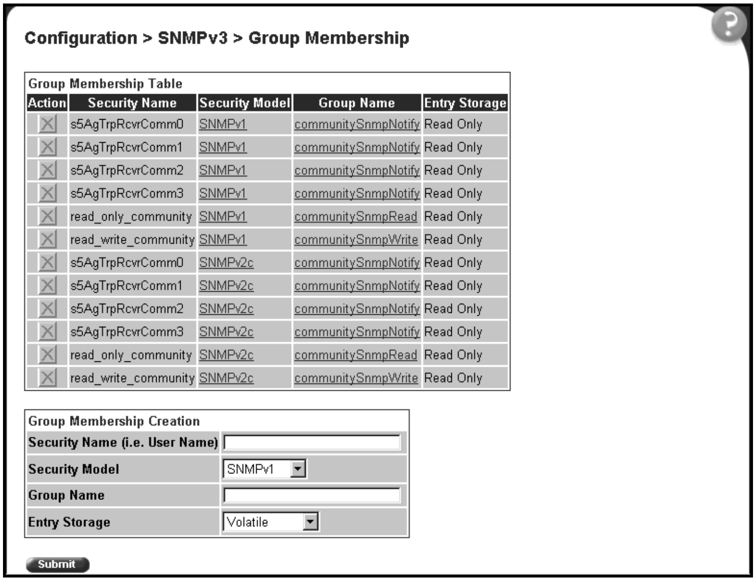
Mapping an SNMPv3 system user to a group

To map an SNMPv3 system user to a group:

1. From the main menu, choose Configuration > SNMPv3 > Group Membership.

   The Group Membership page opens (Figure 21).

Figure 21 Group Membership page



Configuration > SNMPv3 > Group Membership

Group Membership Table

Action	Security Name	Security Model	Group Name	Entry Storage
☒	s5AgTrpRcvrComm0	SNMPv1	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm1	SNMPv1	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm2	SNMPv1	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm3	SNMPv1	communitySnmpNotify	Read Only
☒	read_only_community	SNMPv1	communitySnmpRead	Read Only
☒	read_write_community	SNMPv1	communitySnmpWrite	Read Only
☒	s5AgTrpRcvrComm0	SNMPv2c	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm1	SNMPv2c	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm2	SNMPv2c	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm3	SNMPv2c	communitySnmpNotify	Read Only
☒	read_only_community	SNMPv2c	communitySnmpRead	Read Only
☒	read_write_community	SNMPv2c	communitySnmpWrite	Read Only

Group Membership Creation

Security Name (i.e. User Name)	
Security Model	SNMPv1
Group Name	
Entry Storage	Volatile

Table 19 describes the items on the Group Membership page.

Table 19 Group Membership page items

Item and MIB association	Range	Description
☒		Deletes the row.
Security Name (vacmSecurityToGroupStatus)	1..32	Type a string of character to create a security name for the principal which is mapped by this entry to a group name.
Security Model (vacmSecurityToGroupStatus)	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model within which the security name to group name mapping is valid.
Group Name (vacmGroupName)	1..32	Type a string of character to specify the group name.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2. In the Group Membership Creation section, type information in the text boxes, or select from a list.
3. Click Submit.

   The new entry appears in the Group Membership Table.

Deleting an SNMPv3 group membership configuration

To delete an SNMPv3 group membership configuration:

1. From the main menu, choose Configuration > SNMPv3 > Group Membership.

   The Group Membership page opens (Figure 21).

2. In the Group Membership Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the group membership configuration.
   - Click Cancel to return to the Group Membership page without making changes.

Note: This Group Membership Table section of the Group Membership page contains hyperlinks to the SNMPv3 User Specification and Group Access Rights pages. For more information on these pages, see "Configuring user access to SNMPv3" on page 65 and "Configuring SNMPv3 group access rights" on page 71.

Configuring SNMPv3 group access rights

You can view a table of existing SNMPv3 group access rights configurations, and you can create or delete a group's SNMPv3 system-level access rights.

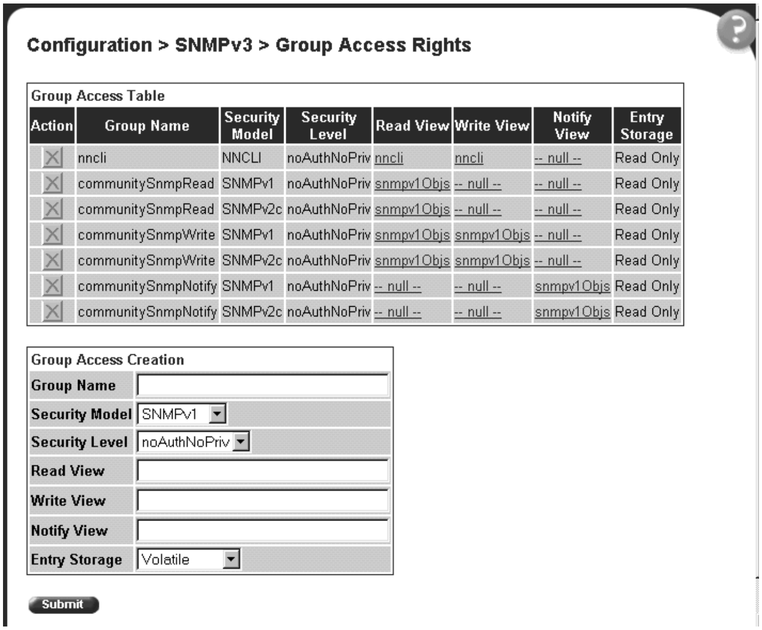
Creating an SNMPv3 group access rights configuration

To create a group's SNMPv3 system-level access right configuration:

1 From the main menu, choose Configuration > SNMPv3 > Group Access Rights.

The Group Access Rights page opens (Figure 22).

Figure 22 Group Access Rights page



Configuration > SNMPv3 > Group Access Rights

Group Access Table

Action	Group Name	Security Model	Security Level	Read View	Write View	Notify View	Entry Storage
☒	nncli	NNCLI	noAuthNoPriv	nncli	nncli	-- null --	Read Only
☒	communitySnmpRead	SNMPv1	noAuthNoPriv	snmpv1Objs	-- null --	-- null --	Read Only
☒	communitySnmpRead	SNMPv2c	noAuthNoPriv	snmpv1Objs	-- null --	-- null --	Read Only
☒	communitySnmpWrite	SNMPv1	noAuthNoPriv	snmpv1Objs	snmpv1Objs	-- null --	Read Only
☒	communitySnmpWrite	SNMPv2c	noAuthNoPriv	snmpv1Objs	snmpv1Objs	-- null --	Read Only
☒	communitySnmpNotify	SNMPv1	noAuthNoPriv	-- null --	-- null --	snmpv1Objs	Read Only
☒	communitySnmpNotify	SNMPv2c	noAuthNoPriv	-- null --	-- null --	snmpv1Objs	Read Only

Group Access Creation

Group Name	
Security Model	SNMPv1
Security Level	noAuthNoPriv
Read View	
Write View	
Notify View	
Entry Storage	Volatile

Table 20 describes the items on the Group Access Rights page.

Table 20 Group Access Rights page items

Item and MIB association	Range	Description
☒		Deletes the row.
Group Name (vacmAccessToGroupStatus)	1..32	Type a character string to specify the group name to which access is granted.
Security Model (vacmAccessSecurityModel)l	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model to which access is granted.
Security Level (vacmAccessSecurityLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the minimum level of security required in order to gain the access rights allowed to the group.
Read View (vacmAccessReadViewName)	1..32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes read access.
Write View (vacmAccessWriteViewName)	1..32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes write access.
Notify View (vacmAccessNotifyViewName)	1..32	Type a character string to identify the MIB view to which this entry authorizes access to notifications.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Group Access Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Group Access Table.

Deleting an SNMPv3 group access rights configuration

To delete a n SNMPv3 group access configuration:

1 From the main menu, choose Configuration > SNMPv3 > Group Access Rights.

The Group Access Rights page opens (Figure 22).

2 In the Group Access Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the group access configuration.
- Click Cancel to return to the Group Access Rights page without making changes.

Note: This Group Access Table section of the Group Access Rights page contains hyperlinks to the Management Information View page. For more information, see "Configuring an SNMPv3 management information view" on page 73.

Configuring an SNMPv3 management information view

You can view a table of existing SNMPv3 management information view configurations, and you can create or delete SNMPv3 management information view configurations.

Note: A view may consist of multiple entries in the table, each with the same view name, but a different view subtree.

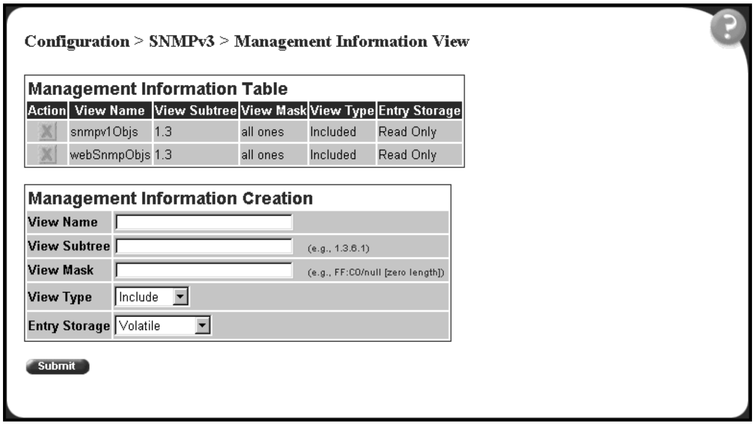
Creating an SNMPv3 management information view configuration

To create an SNMPv3 management information view configuration:

1 From the main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information page opens (Figure 23).

Figure 23 Management Information View page



Configuration > SNMPv3 > Management Information View

Management Information Table

Action	View Name	View Subtree	View Mask	View Type	Entry Storage
☒	snmpv1Objs	1.3	all ones	Included	Read Only
☒	webSnmpObjs	1.3	all ones	Included	Read Only

Management Information Creation

View Name		
View Subtree		(e.g., 1.3.6.1)
View Mask		(e.g., FF:C0/null [zero length])
View Type	Include	
Entry Storage	Volatile	

Table 21 describes the items on the Management Information View page.

Table 21 Management Information View page items

Item and MIB association	Range	Description
☒		Deletes the row.
View Name (vacmViewTreeFamilyViewName)	1..32	Type a character string to create a name for a family of view subtrees.
View Subtree (vacmViewTreeFamilySubtree)	X.X.X.X.X...	Type an object identifier (OID) to specify the MIB subtree which, when combined with the corresponding instance of vacmViewTreeFamilyMask, defines a family of view subtrees. Note: If no OID is entered and the field is blank, a default mask value consisting of “1s” is recognized.
View Mask (vacmViewTreeFamilyMask)	Octet String (0..16)	Type the bit mask which, in combination with the corresponding instance of vacmViewFamilySubtree, defines a family of view subtrees.
View Type (vacmViewTreeFamilyType)	(1) Included (2) Excluded	Choose to include or exclude a family of view subtrees.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Management Information Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Management Information Table (Figure 23).

Deleting an SNMPv3 management information view configuration

To delete an existing SNMPv3 management information view configuration:

1 From the main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information page opens (Figure 23).

2 In the Management Information Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the management information view configuration.
- Click Cancel to return to the table without making changes.

Configuring an SNMPv3 system notification entry

You can view a table of existing SNMPv3 system notification configurations, and you can configure specific SNMPv3 system notification types with particular message recipients and delete SNMPv3 notification configurations.

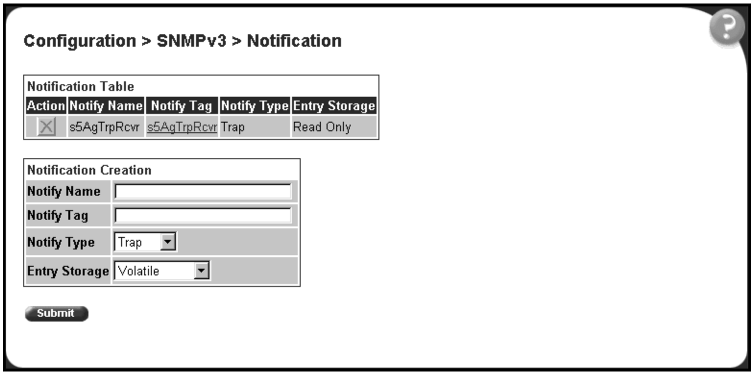
Creating an SNMPv3 system notification configuration

To create an SNMPv3 system notification configuration:

1 From the main menu, choose Configuration > SNMPv3 > Notification.

The Notification page opens (Figure 24).

Figure 24 Notification page



Configuration > SNMPv3 > Notification

Notification Table

Action	Notify Name	Notify Tag	Notify Type	Entry Storage
☒	s5AgTrpRcvr	s5AgTrpRcvr	Trap	Read Only

Notification Creation

Notify Name	
Notify Tag	
Notify Type	Trap
Entry Storage	Volatile

Table 22 describes the items on the Notification page.

Table 22 Notification page items

Item and MIB association	Range	Description
☒		Deletes the row.
Notify Name (snmpNotifyRowStatus)	1..32	Type a character string to identify the entry.
Notify Tag (snmpNotifyTag)	1..32	Type a value which to use to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object carries a zero length, no entries are selected
Notify Type (snmpNotifyType)	(1) Trap (2) Inform	Choose the type of notification to generate.
Entry Storage (snmpNotifyStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Notification Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Notification Table (Figure 24).

Note: This Notification Table section of the Notification page contains hyperlinks to the Target Parameter page. For more information, see "Configuring an SNMPv3 management target parameter" on page 80.

Deleting an SNMPv3 system notification configuration

To delete an SNMPv3 notification configuration:

1 From the main menu, choose Configuration > SNMPv3 > Notification.

The Notification page opens (Figure 24).

2 In the Notification Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the notification configuration.
- Click Cancel to return to the table without making changes.

Configuring an SNMPv3 management target address

You can view a table of existing SNMPv3 management target configurations, create SNMPv3 management target address configurations that associate notifications with particular recipients and delete SNMPv3 target address configurations.

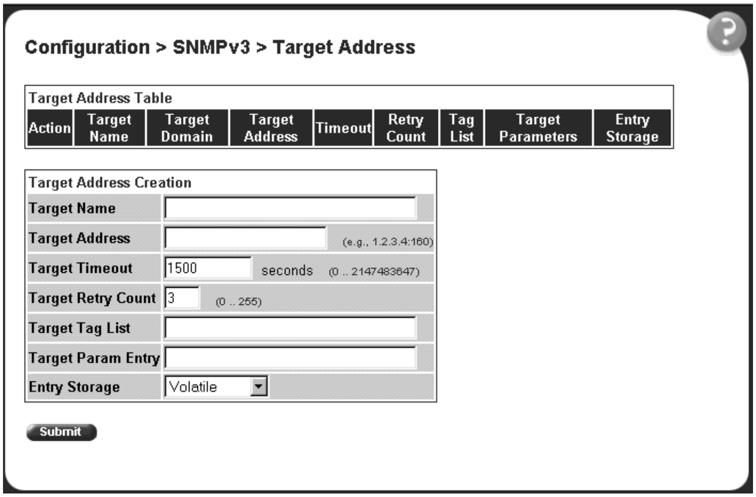
Creating an SNMPv3 target address configuration

To create an SNMPv3 target address configuration:

1 From the main menu, choose Configuration > SNMPv3 > Target Address.

The Target Address page opens (Figure 25).

Figure 25 Target Address page



Configuration > SNMPv3 > Target Address

Target Address Table

Action	Target Name	Target Domain	Target Address	Timeout	Retry Count	Tag List	Target Parameters	Entry Storage

Target Address Creation

Target Name	
Target Address	(e.g., 1.2.3.4:160)
Target Timeout	1500 seconds (0 .. 2147483647)
Target Retry Count	3 (0 .. 255)
Target Tag List	
Target Param Entry	
Entry Storage	Volatile

Table 23 describes the items on the Target Address page.

Table 23 Target Address page items

Item and MIB association	Range	Description
☒		Deletes the row.
Target Name (snmpTargetAddrName)	1..32	Type a character string to create a target name.
Target Domain (snmpTargetAddrTDomain)	1..32	The transport type of the address contained in the snmpTargetAddrTAddress object.
Target Address (snmpTargetAddrTAddress)	XXX.XXX.XXX.XXX:XXX	Type a transport address in the format of an IP address, colon, and UDP port number. For example: 10.30.31.99:162 (see Figure 25 on page 78).
Target Timeout (snmpTargetAddrTimeout)	Integer	Type the number, in seconds, to designate as the maximum time to wait for a response to an inform notification before re-sending the “Inform” notification.
Target Retry Count (snmpTargetAddrRetryCount)	0..255	Type the default number of retires to be attempted when a response is not received for a generated message. An application may provide its own retry count, in which case the value of this object is ignored.
Target Tag List (snmpTargetAddrTagList)	1..20	Type the space-separated list of tag values to be used to select target addresses for a particular operation.
Target Parameter Entry (snmpTargetAddr)	1..32	Type a numeric string to identify an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generated messages to be sent to this transport address
Entry Storage	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Target Address Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Target Address Table (Figure 25).

Note: This Target Address Table section of the Target Address page contains hyperlinks to the Target Parameter page. For more information, see “Configuring an SNMPv3 management target parameter” on page 80.

Deleting an SNMPv3 target address configuration

To delete an SNMPv3 target address configuration:

1. From the main menu, choose Configuration > SNMPv3 > Target Address.

   The Target Address page opens (Figure 25).

2. In the Target Address Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the target address configuration.
   - Click Cancel to return to the table without making changes.

Configuring an SNMPv3 management target parameter

SNMPv3 management target parameters are used during notification generation to specify the communication parameters used for exchanges with notification recipients.

You can view a table of existing SNMPv3 target parameter configurations, create SNMPv3 target parameters that associate notifications with particular recipients, and delete existing SNMPv3 target parameter configurations.

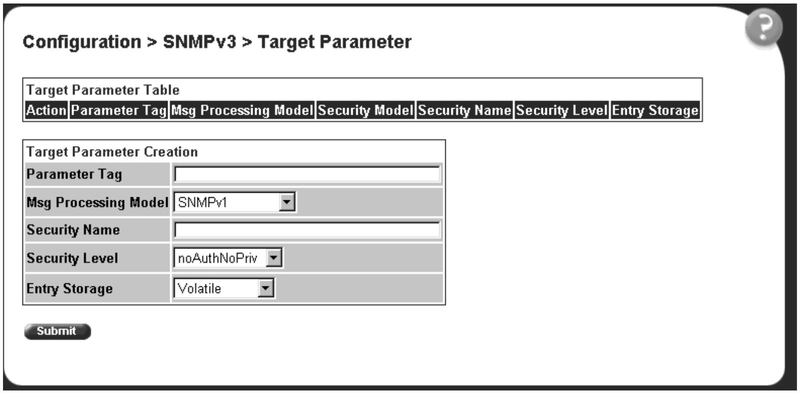
Creating an SNMPv3 target parameter configuration

To create an SNMPv3 target parameter configuration:

1. From the main menu, choose Configuration > SNMPv3 > Target Parameter.

   The Target Parameter page opens (Figure 26).

Figure 26 Target Parameter page



Configuration > SNMPv3 > Target Parameter

Target Parameter Table

Action	Parameter Tag	Msg Processing Model	Security Model	Security Name	Security Level	Entry Storage

Target Parameter Creation

Parameter Tag	
Msg Processing Model	SNMPv1
Security Name	
Security Level	noAuthNoPriv
Entry Storage	Volatile

Table 24 describes the items on the Target Parameter page.

Table 24 Target Parameter page items

Item	Range	Description
☒		Deletes the row.
Parameter Tag (snmpTargetParamsRowStatus)	1..32	Type a unique character string to identify the parameter tag.
Msg Processing Model (snmpTargetParamsMPModel)	(0) SNMPv1 (1) SNMPv2c (2) SNMPv2* (3) SNMPv3 /USM	Choose the message processing model to be used when generating SNMP messages using this entry.
Security Name (snmpTargetParamsSecuirtyName)	1..32	Type the principal on whose behalf SNMP messages are generated using this entry
Security Level (snmpTargetParamsSecuirtyLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the level of security to be used when generating SNMP messages using this entry
Entry Storage (snmpTargetParamsStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Target Parameter Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Target Parameter Table (Figure 26).

Deleting an SNMPv3 target parameter configuration

To delete an SNMPv3 target parameter configuration:

1. From the main menu, choose Configuration > SNMPv3 > Target Address.

   The Target Address page opens (Figure 25).

2. In the Target Parameter Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the target parameter configuration.
   - Click Cancel to return to the table without making changes.

Configuring SNMP traps

You can configure the IP address and community string for a new SNMP trap receiver, view a table of existing SNMP trap receiver configurations, or delete an existing SNMP trap receiver configuration(s).

➡ **Note:** The SNMP Trap Receiver Table is an alternative to using the SNMPv3 Target Table and SNMPv3 Parameter Table. However, only SNMPv1 traps are configurable using this table.

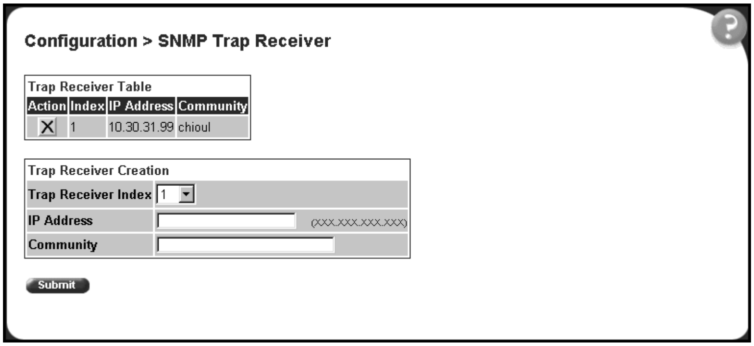
Creating an SNMP trap receiver configuration

To create an SNMP trap receiver configuration:

1. From the main menu, choose Configuration > SNMP Trap.

   The SNMP Trap Receiver page opens (Figure 27).

Figure 27 SNMP Trap Receiver page



Configuration > SNMP Trap Receiver

Trap Receiver Table

Action	Index	IP Address	Community
☒	1	10.30.31.99	chioul

Trap Receiver Creation

Trap Receiver Index	1 ▾
IP Address	(XXX.XXX.XXX.XXX)
Community	

Table 25 describes the items on the Trap Receiver Table and Trap Receiver Creation sections of the SNMP Trap Receiver page.

Table 25 SNMP Trap Receiver page items

Items	**Range**	**Description**
☒		Deletes the row.
Trap Receiver Index	1..4	Choose the number of the trap receiver to create or modify.
IP Address	XXX.XXX.XXX.XXX	Type the network address for the SNMP manager that is to receive the specified trap.
Community	0..32	Type the community string for the specified trap receiver.

2 In the Trap Receiver Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Trap Receiver Table (Figure 27).

Deleting an SNMP trap receiver configuration

To delete SNMP trap receiver configurations:

1 From the main menu, choose Configuration > SNMP Trap.

The SNMP Trap Receiver page opens (Figure 27).

2. In the Trap Receiver Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the SNMP trap receiver configuration.
   - Click Cancel to return to the table without making changes.

Configuring EAPOL-based security

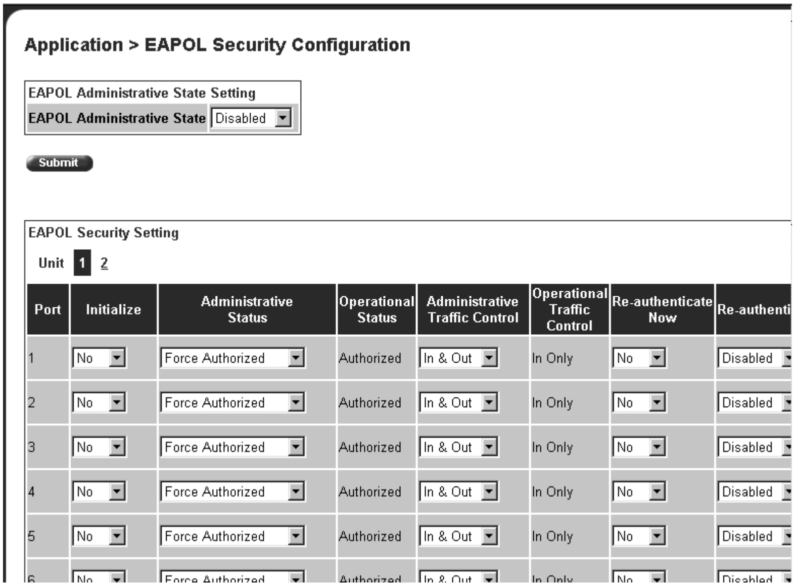
Beginning with software version 1.1, you can configure security based on the Extensible Authentication Protocol over LAN (EAPOL) protocol. Refer to *Using the Business Policy Switch 2000 Software Version 1.2***,** for more information EAPOL-based security.

To configure EAPOL:

1. From the main menu, choose Application > EAPOL Security.

   The EAPOL Security Configuration page opens (Figure 28 and Figure 29). Use the scroll bar on the right to move down the page and the scroll bar on the bottom to move across the page.

Figure 28 EAPOL Security Configuration page (1 of 2)



Application > EAPOL Security Configuration

EAPOL Administrative State Setting

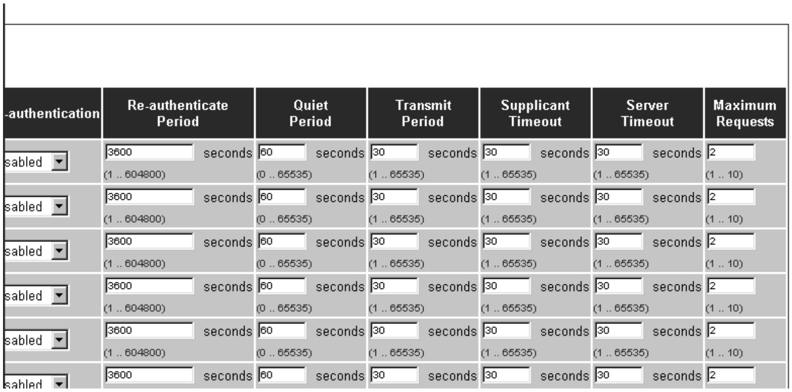
EAPOL Administrative State: Disabled

EAPOL Security Setting

Unit **1** 2

Port	Initialize	Administrative Status	Operational Status	Administrative Traffic Control	Operational Traffic Control	Re-authenticate Now	Re-authenti
1	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
2	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
3	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
4	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
5	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
6	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled

Figure 29 EAPOL Security Configuration page (2 of 2)



-authentication	Re-authenticate Period	Quiet Period	Transmit Period	Supplicant Timeout	Server Timeout	Maximum Requests
sabled	3600 seconds (1 .. 604800)	60 seconds (0 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	2 (1 .. 10)
sabled	3600 seconds (1 .. 604800)	60 seconds (0 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	2 (1 .. 10)
sabled	3600 seconds (1 .. 604800)	60 seconds (0 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	2 (1 .. 10)
sabled	3600 seconds (1 .. 604800)	60 seconds (0 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	2 (1 .. 10)
sabled	3600 seconds (1 .. 604800)	60 seconds (0 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	2 (1 .. 10)
sabled	3600 seconds	60 seconds	30 seconds	30 seconds	30 seconds	2

Table 26 describes the fields on the EAPOL Security Configuration page.

Table 26 EAPOL Security Configuration page fields

Section	Item	Range	Description
EAPOL Administrative State Setting	EAPOL Administrative State	(1) Enabled (2) Disabled	Enables or disables EAPOL-based security.
EAPOL Security Setting	Unit		Displays the unit you are viewing.
	Port	1 to 28	Displays the port number.
	Initialize	(1) Yes (2) No	Activates EAPOL state on this port.
	Administrative Status	(1) Force Unauthorized (2) Auto (3) Force Authorized	Allows you to set the EAPOL authorization status: • Force Unauthorized—Always unauthorized • Auto—Status depends on EAP authentication results • Force Authorized—Always authorized
	Operational Status	(1) Authorized (2) Unauthorized	Displays the current authorization status.
	Administrative Traffic Control	(1) In & Out (2) In Only	Allows you to set EAPOL authentication either for incoming and outgoing traffic or for incoming traffic only.
	Operational Traffic Control	(1) In & Out (2) In Only	Displays the current administrative traffic control setting.
	Re-authenticate Now	(1) Yes (2) No	Allows you to activate EAPOL authentication immediately, without waiting for the re-authentication period to expire.
	Re-authentication	(1) Enabled (2) Disabled	Allows you to repeat EAPOL authentication according to the time value specified in Re-authentication Period field.
	Re-authentication Period	1..604800	With Re-authentication enabled, allows you to specify the time period between successive EAPOL authentications.
	Quiet Period	0..65535	Allows you to specify the time interval between an authentication failure and the start of a new authentication attempt.
	Transmit Period	1..65535	Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets.
	Supplicant Timeout	1..65535	Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets.
	Server Timeout	1..65535	Allows you to specify how long the switch wits for the RADIUS server to respond to all EAP packets.
	Maximum Requests	1..10	Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant.

2. Complete fields as described in the table.
3. Click Submit.

Managing remote access by IP address

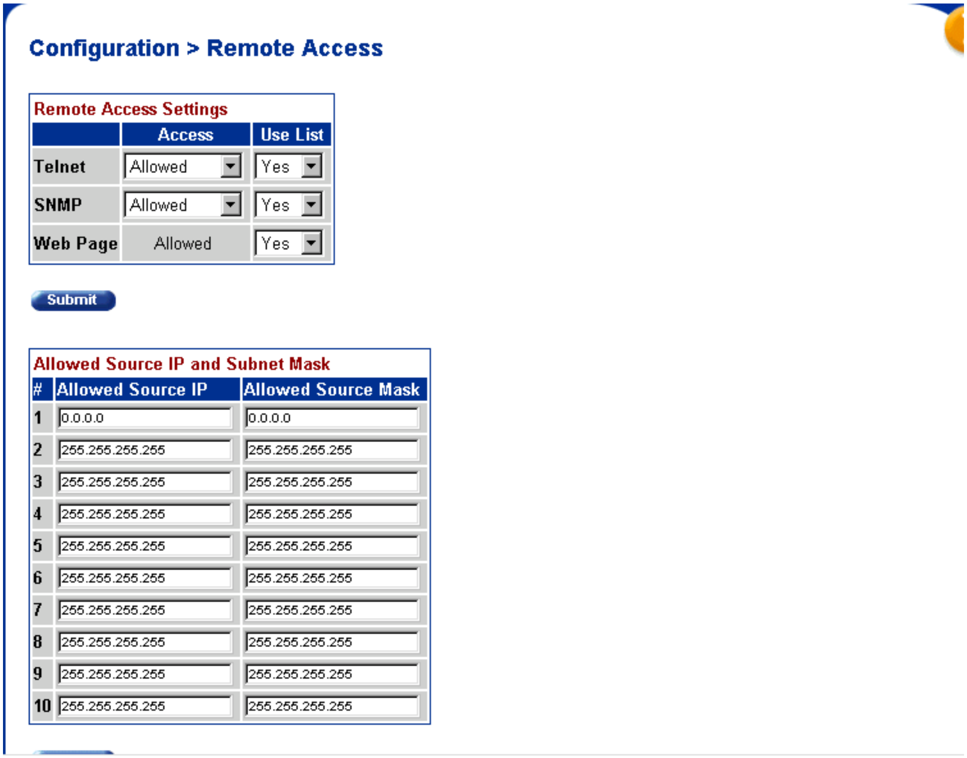
Beginning with software version 1.2, you can configure the remote access you allow. You can specify up to 10 IP addresses to allow Web access, SNMP access, or Telnet access to the BPS 2000.

To configure remote access using the Web-based management system:

1. From the main menu of the Business Policy Switch 2000 Web-based Manager, choose Configuration > Remote Access.

   The Remote Access page opens (Figure 30).

Figure 30 Remote Access page



Configuration > Remote Access

Remote Access Settings

	Access	Use List
Telnet	Allowed	Yes
SNMP	Allowed	Yes
Web Page	Allowed	Yes

Allowed Source IP and Subnet Mask

#	Allowed Source IP	Allowed Source Mask
1	0.0.0.0	0.0.0.0
2	255.255.255.255	255.255.255.255
3	255.255.255.255	255.255.255.255
4	255.255.255.255	255.255.255.255
5	255.255.255.255	255.255.255.255
6	255.255.255.255	255.255.255.255
7	255.255.255.255	255.255.255.255
8	255.255.255.255	255.255.255.255
9	255.255.255.255	255.255.255.255
10	255.255.255.255	255.255.255.255

Table 27 describes the fields on the Remote Access page.

Table 27 Remote Access page fields

Section	Item	Range	Description
Remote Access Settings	Telnet/Access	(1)Allowed (2) Disallowed	Allows Telnet access.
	Telnet/Use List	(1) Yes (2) No	Restricts Telnet access to the specified 10 source IP addresses.
	SNMP/Access	(1)Allowed (2) Disallowed	Allows SNMP access.
	SNMP/Use List	(1) Yes (2) No	Restricts SNMP access to the specified 10 source IP addresses.
	Web Page/Access		Displays allowed Web access.

Table 27 Remote Access page fields (continued)

Section	Item	Range	Description
	Web/Use List	(1) Yes (2) No	Restricts Web access to the specified 10 source IP addresses.
Allowed Source IP and Subnet Mask	Allowed Source IP	XXX.XXX.XXX.XXX	Enter the source IP address you want to allow switch access.
	Allowed Source Mask	XXX.XXX.XXX.XXX	Enter the source IP mask you want to allow switch access.

2 Complete fields as described in the table.

3 Click Submit.

Configuring MAC address-based security

Beginning with software version 1.1, the MAC address-based security system allows you to specify a range of system responses to unauthorized network access to your switch with the Web-based management system.

The system response can range from sending a trap to disabling the port. The network access control is based on the MAC addresses of the authorized stations. You can specify a list of up to 448 MAC addresses that are authorized to access the switch. You can also specify the ports that each MAC address is allowed to access. The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, and so forth. You must also include the MAC address of any router connected to any secure ports.

When the switch software detects a security violation, the response can be to send a trap, turn on destination address (DA) filtering, disable the specific port, or any combination of these three options.

Note: After configuring the switch for MAC address-based security, you must enable the ports you want, using the Port Configuration page.

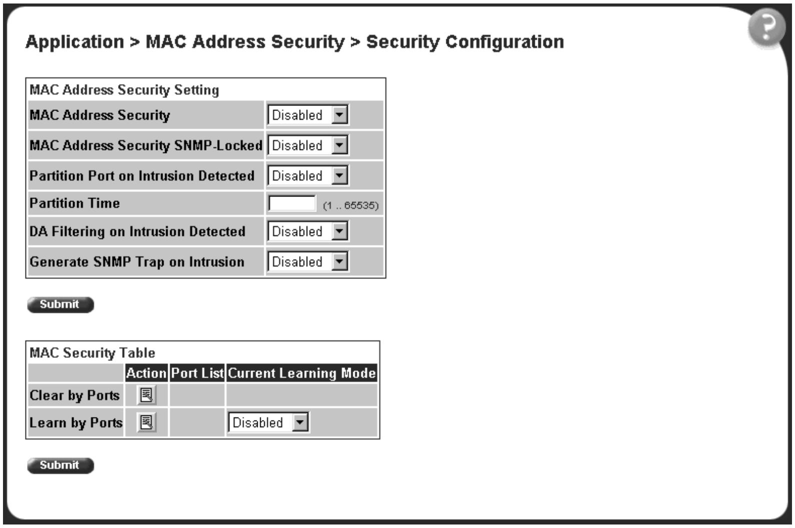
Configuring MAC address-based security

To configure MAC address-based security using the Web-based management system:

1 From the main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 31).

Figure 31 Security Configuration page



Application > MAC Address Security > Security Configuration

MAC Address Security Setting	
MAC Address Security	Disabled
MAC Address Security SNMP-Locked	Disabled
Partition Port on Intrusion Detected	Disabled
Partition Time	(1 .. 65535)
DA Filtering on Intrusion Detected	Disabled
Generate SNMP Trap on Intrusion	Disabled

MAC Security Table

	Action	Port List	Current Learning Mode
Clear by Ports			
Learn by Ports			Disabled

Table 28 describes the items on the Security Configuration page.

Table 28 Security Configuration page items

Section	Item	Range	Description
MAC Address Security Setting	MAC Address Security	(1) Enabled (2) Disabled	Enables the MAC address security features.
	MAC Address Security SNMP-Locked	(1) Enabled (2) Disabled	Enables locking SNMP, so that you cannot use SNMP to modify the MAC address security features.
	Partition Port on Intrusion Detected	(1) Forever (2) Enabled (3) Disabled	Configures how the switch reacts to an intrusion event: • Forever—The port is disabled and remains disabled (partitioned) until reset. The port does not reset after the Partition Time elapses. • Enabled—The port is disabled, then automatically reset to enabled after the time specified in the Partition Time field elapses. • Disabled—The port remains enabled, even if an intrusion event is detected.
	Partition Time	1 to 65535	Sets the time to partition a port on intrusion. Note: Use this field only if the Partition Port on Intrusion Detected field is set to Enabled.
	DA Filtering on Intrusion Detected	(1) Enabled (2) Disabled	Enables you to isolate the intruding node (discard) the packets.
	Generate SNMP Trap on Intrusion	(1) Enabled (2) Disabled	Enables generation of an SNMP when an intrusion is detected.
MAC Security Table/ Clear by Ports	Action	📝	Allows you to clear specific ports from participation in the MAC address security features.
	Port List		Will be blank.
	Current Learning Mode		Will be blank.
MAC Security Table/ Learn by Ports	Action	📝	Allows you to identify ports that will learn incoming MAC addresses. All source MAC addresses of any packets received on a specified port(s) are added to the MAC Security Table (maximum of 448 MAC addresses allowed).
	Port List		Displays all the ports that will learn incoming MAC address to detect intrusions (unallowed MAC addresses).
	Current Learning Mode	(1) Enabled (2) Disabled	Enables learning.

2 On the Security Configuration page, type information in the text boxes, or select from a list.

3 Click Submit.

Configuring ports

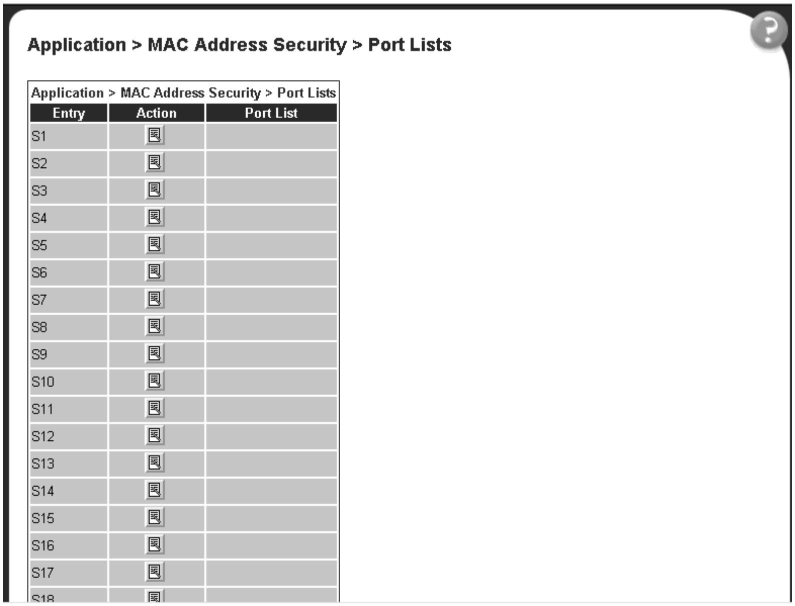
In this section, you create a list of ports, and you can add ports to or delete ports from each list.

To activate an entry or add or delete ports to a list:

1 From the main menu, choose Application > MAC Address Security > Port Lists.

The Port Lists page opens (Figure 32).

Figure 32 Port Lists page



Application > MAC Address Security > Port Lists

Application > MAC Address Security > Port Lists

Entry	Action	Port List
S1	🗎	
S2	🗎	
S3	🗎	
S4	🗎	
S5	🗎	
S6	🗎	
S7	🗎	
S8	🗎	
S9	🗎	
S10	🗎	
S11	🗎	
S12	🗎	
S13	🗎	
S14	🗎	
S15	🗎	
S16	🗎	
S17	🗎	
S18	🗎	

Table 29 describes the items on the Ports Lists page.

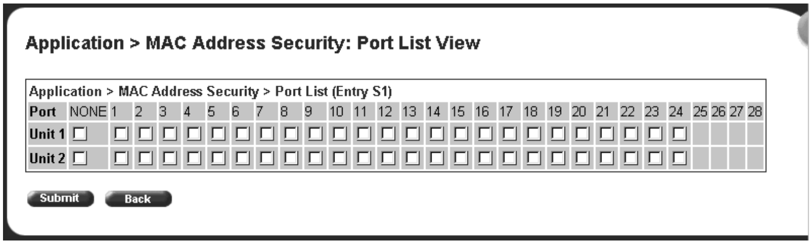
Table 29 Ports Lists page items

Item	Range	Description
Entry		These are the lists of ports.
Action	📝	Allows you to add or delete ports to the lists.
Port List		Displays which ports are associated with each list.

2 To add or delete ports to a list, click the icon in the Action column in the list row you want.

The Port List View, Port List page opens (Figure 33).

Figure 33 Port List View, Port List page



Application > MAC Address Security: Port List View

Application > MAC Address Security > Port List (Entry S1)

Port	NONE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				

a Click the ports you want to add to the selected list or click None.

b To delete a port from a list, uncheck the box by clicking it.

c Click Submit.

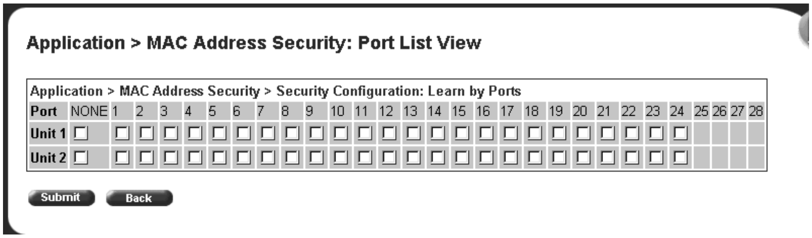
3 From the main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 31).

4 In the MAC Security Table section, click the icon in the Action column of the Learn By Ports row.

The Port List View, Learn by Ports page opens (Figure 34).

Figure 34 Port List View, Learn by Ports page



Application > MAC Address Security: Port List View

Application > MAC Address Security > Security Configuration: Learn by Ports

Port	NONE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				

- **a** Click the ports through which you want the switch to learn MAC addresses or click None.
- **b** If you want that port to no longer learn MAC addresses, click the checked box to uncheck it.
- **c** Click Submit.

5 In the MAC Security Table section, choose Enabled in the Current Learning Mode column of the Learn By Ports row.

6 Click Submit.

Note: You cannot include any of the port values you have chosen for the secure ports field.

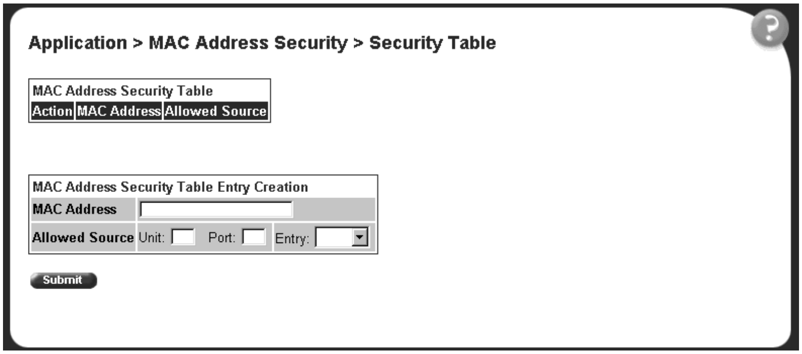
Adding MAC addresses

To add MAC address to the MAC address-based security system:

1 In the main menu, choose Applications > MAC Address Security > Security Table.

It may take awhile for the required addresses to be learned. Then, the Security Table page opens (Figure 35).

Figure 35 Security Table page



Application > MAC Address Security > Security Table

MAC Address Security Table

Action	MAC Address	Allowed Source

MAC Address Security Table Entry Creation

MAC Address	
Allowed Source	Unit: Port: Entry:

Note: Using this page, you instruct the switch to allow the specified MAC address access *only* through the specified port or port list.

Table 30 describes the items on the Security Table page.

Table 30 Security Table page items

Section	Item	Range	Description
MAC Address Security Table	Action	☒	Allows you to delete a MAC address.
	Address		Displays the MAC address.
	Allowed Source	(1) Unit/Port (2) Entry	Displays the entry through which the MAC address is allowed.
MAC Address Security Table Entry Creation	MAC Address		Enter the MAC address you want to allow to access the switch.
	Allowed Source		Select the unit and port through which the MAC address is allowed.
	Entry		Select the port list through which the MAC address is allowed.

2 Complete fields as described in the table.

Note: If you choose an Entry as the Allowed Source, you must have configured that specific entry on the Port View List, Port List page.

3 On the Security Table page, type information in the text boxes, or select from a list.

4 Click Submit.

Note: Be certain to include the MAC address for the default LAN router as an allowed source MAC address.

Clearing ports

You can clear all information from the specified port(s) for the list of ports that learn MAC addresses. If Learn by Ports is enabled, the specified ports will begin again to learn the MAC addresses.

To clear information from selected ports:

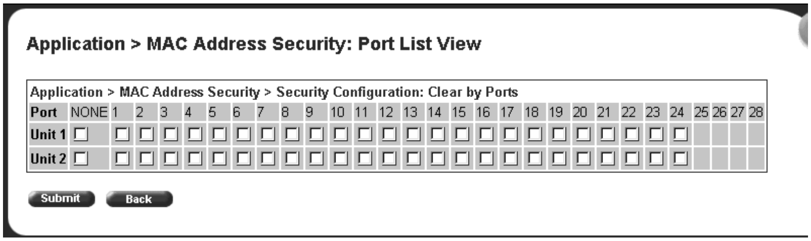
1 From the main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 31).

2 In the MAC Security Table section, click the icon in the Action column of the Clear By Ports row.

The Port List View, Clear by Ports page opens (Figure 36).

Figure 36 Port List View, Clear by Ports page



Application > MAC Address Security: Port List View

Application > MAC Address Security > Security Configuration: Clear by Ports

Port	NONE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				

3 Select the ports you want to clear or click None.

4 Click Submit.

Note: When you specify a port (or ports) to be cleared using this field, the specific port (or ports) will be cleared for each of the entries listed in the MAC Address Security Table. If you totally clear the allowed Source Port(s) field (leaving a blank field) for an entry, the associated MAC address for that entry is also cleared.

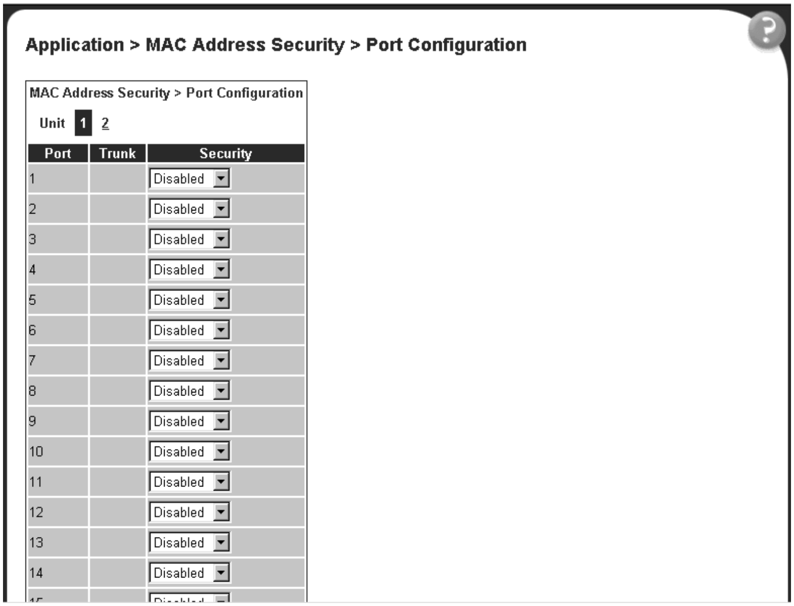
Enabling security on ports

To enable or disable MAC address-based security on the port:

1 From the main menu, choose Application > MAC Address Security > Port Configuration.

The Port Configuration page opens (Figure 37).

Figure 37 Port Configuration page



Application > MAC Address Security > Port Configuration

MAC Address Security > Port Configuration

Unit **1** 2

Port	Trunk	Security
1		Disabled
2		Disabled
3		Disabled
4		Disabled
5		Disabled
6		Disabled
7		Disabled
8		Disabled
9		Disabled
10		Disabled
11		Disabled
12		Disabled
13		Disabled
14		Disabled

Table 31 describes the items on the Port Configuration page.

Table 31 Port Configuration page items

Item	Range	Description
Unit	1 to 8	Displays the unit number of the ports shown in the table.
Port	1 to 28	Lists each port on the unit.
Trunk	Blank, 1 to 6	Displays the MultiLink Trunk that the port belongs to.
Security	(1) Enabled (2) Disabled	Enables MAC address-based security on that port. Note: You must configure the port for MAC address-based security before enabling the security.

Deleting ports

You can delete ports from the security system in a variety of ways:

- In the Ports List View, Port List page (Figure 33), click on the checkmark of a selected port to delete that port from the specified port list.

- In the Ports List View, Learn by Ports page (Figure 34), click on the checkmark of a selected port to remove that port from those that learn MAC addresses.
- In the Port Configuration page (Figure 37), click Disabled to remove that port from the MAC address-based security system; it will disable all MAC address-based security on that port.

Viewing learned MAC addresses by VLAN

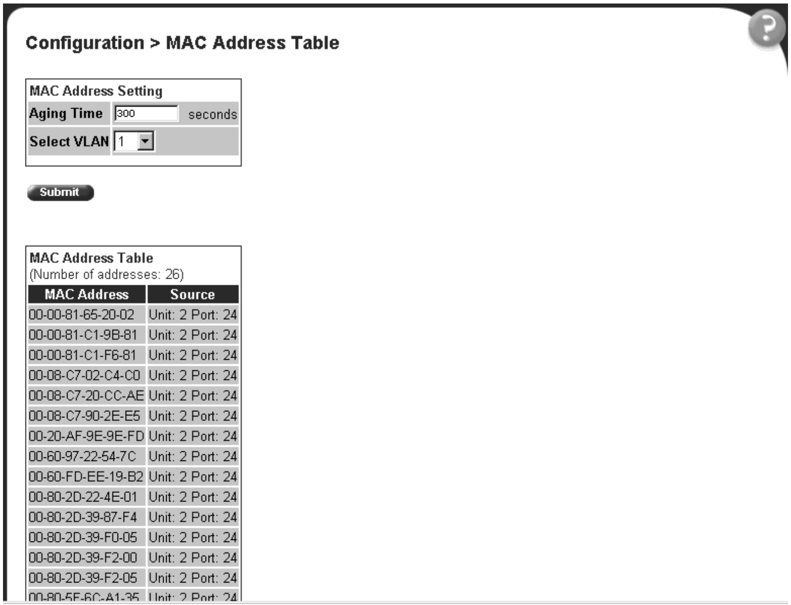
You can view MAC addresses and their associated port or trunk that the switch or stack configuration has learned, based on the VLAN you select.

To view learned MAC addresses and their associated port or trunk:

1 From the main menu, choose Configuration > MAC Address Table.

The MAC Address Table page opens (Figure 38).

Figure 38 MAC Address Table page



MAC Address Setting

Aging Time 300 seconds

Select VLAN 1

MAC Address Table
(Number of addresses: 26)

MAC Address	Source
00-00-81-65-20-02	Unit: 2 Port: 24
00-00-81-C1-9B-81	Unit: 2 Port: 24
00-00-81-C1-F6-81	Unit: 2 Port: 24
00-08-C7-02-C4-C0	Unit: 2 Port: 24
00-08-C7-20-CC-AE	Unit: 2 Port: 24
00-08-C7-90-2E-E5	Unit: 2 Port: 24
00-20-AF-9E-9E-FD	Unit: 2 Port: 24
00-60-97-22-54-7C	Unit: 2 Port: 24
00-60-FD-EE-19-B2	Unit: 2 Port: 24
00-80-2D-22-4E-01	Unit: 2 Port: 24
00-80-2D-39-87-F4	Unit: 2 Port: 24
00-80-2D-39-F0-05	Unit: 2 Port: 24
00-80-2D-39-F2-00	Unit: 2 Port: 24
00-80-2D-39-F2-05	Unit: 2 Port: 24
00-80-5F-6C-A1-35	Unit: 2 Port: 24

Table 32 describes the items on the MAC Address Table page.

Table 32 MAC Address Table page items

Section	Item	Range	Description
MAC Address Setting	Aging Time	10..1000000	Type the timeout period, in seconds, for aging out dynamically learned forwarding information. If the entry is inactive for a period of time that exceeds the specified aging time, the address is removed. Note: Nortel Networks recommends that you use the default value of 300 seconds.
	Select VLAN	1..256	Choose the VLAN on which to view learned MAC addresses.
MAC Address Table	MAC Address		The unicast MAC address for which the bridge has forwarding and/or filtering information.
	Source		The source of the discovered MAC address.

2 In the MAC Address Setting section, choose the aging time and VLAN you want to view learned MAC addresses on.

3 Click Submit.

Your request is displayed in the MAC Address Table (Figure 38).

Locating a specific MAC address

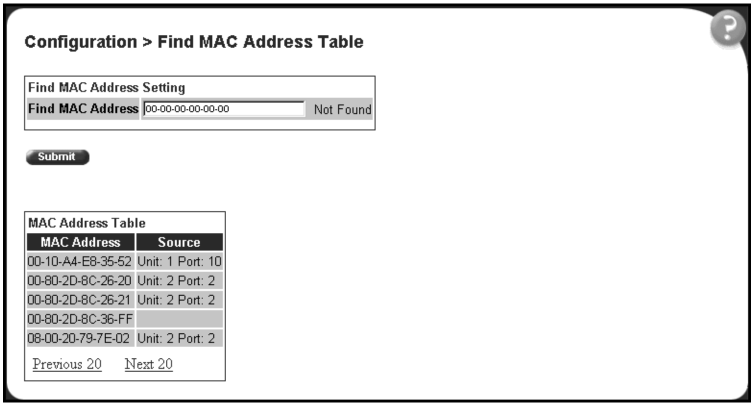
You can search for a specific MAC address among all the MAC addresses learned from all the VLANs. This is a useful tool for finding whether or not a switch has learned a particular address.

To locate a specific MAC addresses:

1 From the main menu, choose Configuration > Find MAC Address.

The Find MAC Address page opens (Figure 39).

Figure 39 Find MAC Address Table page



Configuration > Find MAC Address Table

Find MAC Address Setting

Find MAC Address	00-00-00-00-00-00	Not Found

MAC Address Table

MAC Address	Source
00-10-A4-E8-35-52	Unit: 1 Port: 10
00-80-2D-8C-26-20	Unit: 2 Port: 2
00-80-2D-8C-26-21	Unit: 2 Port: 2
00-80-2D-8C-36-FF	
08-00-20-79-7E-02	Unit: 2 Port: 2

Table 32 on page 100 describes the items on the Find MAC Address Table page.

2 In the MAC Address Setting section, type the MAC address you want to search for.

3 Click Submit to enter the request.

If the address is located, it is shown in the first row in the MAC Address Table section. If the address is not located, the system response “Not Found” is shown to the right of the Find MAC Address input field.

Configuring switch port autonegotiation speed

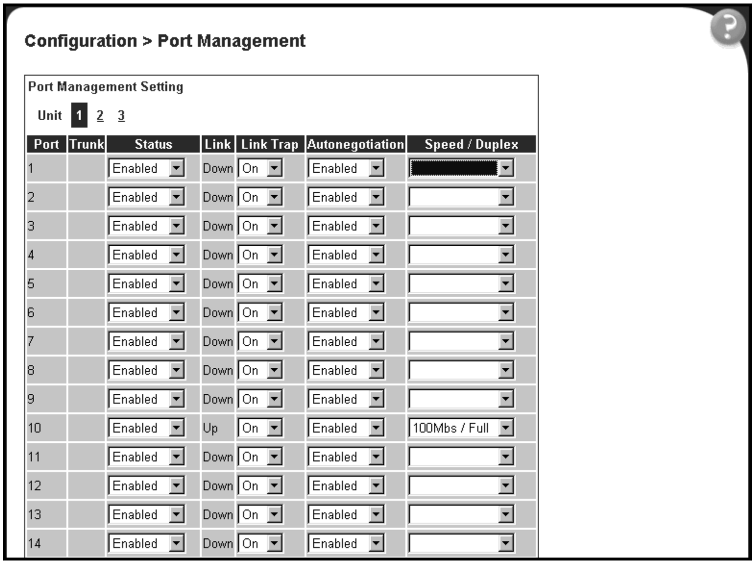
You can configure a specific switch port or all switch ports to autonegotiate for the highest available speed of the connected station or you can set the speed for selected switch ports (autonegotiation is not supported on 100 Mbps fiber optic ports).

To configure a switch port's autonegotiation speed:

1. From the main menu, choose Configuration > Port Management.

   The Port Management page opens (Figure 40).

Figure 40 Port Management page



Configuration > Port Management

Port Management Setting

Unit **1** 2 3

Port	Trunk	Status	Link	Link Trap	Autonegotiation	Speed / Duplex
1		Enabled	Down	On	Enabled	
2		Enabled	Down	On	Enabled	
3		Enabled	Down	On	Enabled	
4		Enabled	Down	On	Enabled	
5		Enabled	Down	On	Enabled	
6		Enabled	Down	On	Enabled	
7		Enabled	Down	On	Enabled	
8		Enabled	Down	On	Enabled	
9		Enabled	Down	On	Enabled	
10		Enabled	Up	On	Enabled	100Mbs / Full
11		Enabled	Down	On	Enabled	
12		Enabled	Down	On	Enabled	
13		Enabled	Down	On	Enabled	
14		Enabled	Down	On	Enabled	

Table 33 describes the items on the Port Management page.

Table 33 Port Management page items

Item	Range	Description
Port		The switch port number of the corresponding row. To select the switch row, click the check box to the right. The values that you set in each switch row affect all switch ports and, when the switch is part of a stack, the values that set in the stack row affect all ports in the entire stack (except the gigabit media dependent adaptor (MDA) ports or fiber optic ports when installed). For information on setting high speed flow control for MDAs, see "Configuring high speed flow control" on page 104.
Trunk		The trunk group that the switch port belongs to as specified in the Trunk Member fields on the MultiLink Trunk page. For more information, see "Configuring MultiLink Trunk (MLT) members" on page 186.
Status	(1) Enabled (2) Disabled	Choose to enable or disable the port. You can also use this field to control access to any switch port. The default setting is Enabled.
Link		The current link state of the corresponding port as follows: • Up: The port is connected and operational • Down: The port is not connected or is not operational.
Link/Trap	(1) On (2) Off	Choose to control whether link up/down traps are sent to the configured trap sink from the switch. The default setting is On.
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. Choosing to enable autonegotiation sets the corresponding port speed to match the best service provided by the connected station, up to 100Mb/s in full-duplex mode. Note: This field is disabled for all fiber optic ports other than gigabit fiber optic ports. The default setting is Enabled.
Speed / Duplex	(1) 10Mbs / Half (2) 10Mbs / Full (3) 100Mbs / Half (4) 100Mbs / Full (5) 1000Mbs / Full	Choose the Ethernet speed you want the port to support. Note: Fiber optic ports can only be set to 100 Mb/s/Half or 100 Mb/s/Full. The default setting is 100Mbs/Half when autonegotiation is disabled and 1000 Mb/s full-duplex for gigabit ports only.
	Note: Disabling ports that are trunk members automatically disables all ports within that trunk.	

2. In the upper-left hand corner, click on the unit number of the policy switch to manage.

   The page is updated with the information for the selected switch.

3. In the port row of your choice, select from the lists.
4. Click Submit.

Configuring high speed flow control

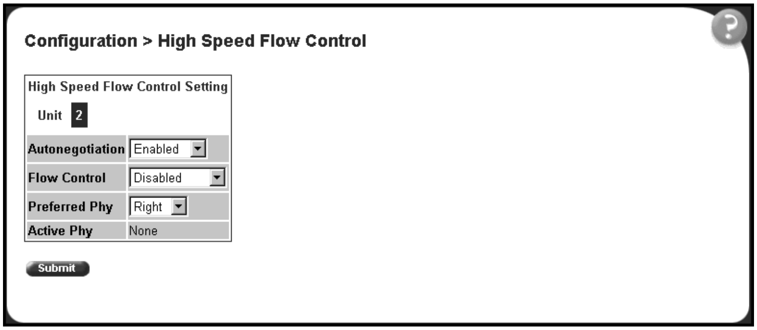
You can set switch port parameters for Gigabit Ethernet media dependent adapters (MDAs) when the switch is participating in a stack configuration.

To configure high speed flow control:

1. From the main menu, choose Configuration > High Speed Flow Control.

   The High Speed Flow Control page opens (Figure 41).

Figure 41 High Speed Flow Control page



Configuration > High Speed Flow Control

High Speed Flow Control Setting

Unit 2

Autonegotiation	Enabled
Flow Control	Disabled
Preferred Phy	Right
Active Phy	None

Table 34 describes the items on the High Speed Flow Control page.

Table 34 High Speed Flow Control page items

Item	Range	Description
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. When enabled, the port advertises support for flow control autonegotiation.
Flow Control	(1) Enabled (2) Symmetric (3) Asymmetric	Choose your flow control preference to control traffic and avoid congestion on the gigabit MDA port. Note: Ensure that the settings are the same for both sides of the link.
Preferred Phy	(1) Left (2) Right	Choose the preferred physical port. The port not selected automatically reverts to a backup physical port.
Active Phy		The current operating physical port. The physical port options are left or right.

2. In the upper-left hand corner, click on the unit number of the gigabit MDA to configure.
3. Select from the lists.
4. Click Submit.

Downloading switch images

You can download the BPS 2000 software image that is located in non-volatile flash memory. To download the BPS 2000 software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the policy switch must have an IP address. To learn how to configure the switch or stack IP address, refer to "Configuring BootP, IP, and gateway settings" on page 58.

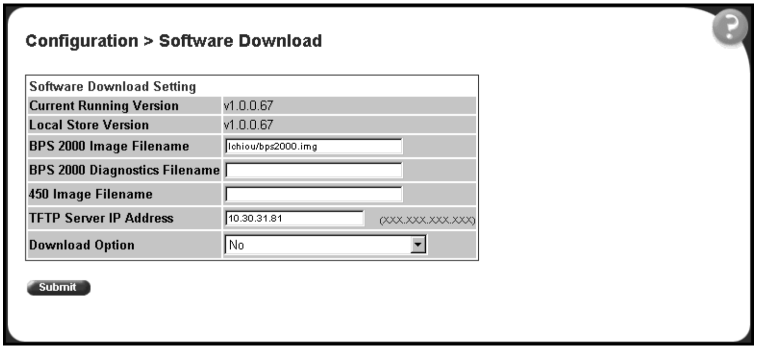
Caution: Do not interrupt power to the device during the software download process. A power interruption can corrupt the firmware image.

To download a switch image:

1 From the main menu, choose Configuration > Software Download.

The Software Download page opens (Figure 42).

Figure 42 Software Download page



Configuration > Software Download

Software Download Setting	
Current Running Version	v1.0.0.67
Local Store Version	v1.0.0.67
BPS 2000 Image Filename	lchiou/bps2000.img
BPS 2000 Diagnostics Filename	
450 Image Filename	
TFTP Server IP Address	10.30.31.81 (XXX.XXX.XXX.XXX)
Download Option	No

Table 35 describes the items on the Software Download page.

Table 35 Software Download page items

Item	Range	Description
Current Running Version		The version of the current running software.
Local Store Version		The local version of the software in the flash memory.
BPS 2000 Image Filename	1..30	Type the software image load filename.
BPS 2000 Diagnostics Filename	1..30	Type the diagnostics filename.
450 Image Filename	1..30	Type the 450 image filename.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of your TFTP load host.
Download Option	(1) No (2) BPS 2000 Image (3) BPS 200 Diagnostics (4) 450/410 Image (5) BPS 2000 and 450/410 Images	Choose the software image to load.

2. Type information in the text boxes, or select from a list.
3. Click Submit.

The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Take care not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

When the download process is complete, the switch automatically resets and the new software image initiates a self-test.

During the download process, the Business Policy Switch is not operational. You can monitor the progress of the download process by observing the LED indications.

Table 36 describes the LED indications during the software download process.

Note: The LED indications described in Table 36 apply to a 24-port switch model. Although a 12-port switch provides *similar* LED indications, the LED indication sequence is associated within the 12-port range.

Table 36 LED Indications during the software download process

Phase	Description	LED Indications
1	The switch downloads the new software image.	**100 Mb/s port status LEDs (ports 18 to 24 only):** The LEDs begin to turn on in succession beginning with port 24, which indicates the progress of the download process. When LEDs 18 to 24 are all on, the switch has received the new software image successfully.
2	The switch erases the flash memory.	**100 Mb/s port status LEDs (ports 1 to 12 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that various sectors of the switch's flash memory are being erased. When LEDs 1 to 12 are all on, the switch's flash memory has been erased.

Table 36 LED Indications during the software download process (continued)

Phase	Description	LED Indications
3	The switch programs the new software image into the flash memory.	**100 Mb/s port status LEDs (ports 1 to 8 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that the new software image is being programmed into the switch's flash memory. When LEDs 1 to 8 are all on, the new software image has been programmed successfully into the switch's flash memory.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

Storing and retrieving a switch configuration file from a TFTP server

You can store switch and stack configuration parameters on a Trivial File Transfer Protocol (TFTP) server. You can retrieve the configuration parameters of a standalone switch or an entire stack and use the retrieved parameters to automatically configure a replacement switch or stack.

To store a switch or stack configuration, you must set up the file on your TFTP server and set the filename read/write permission to enabled.

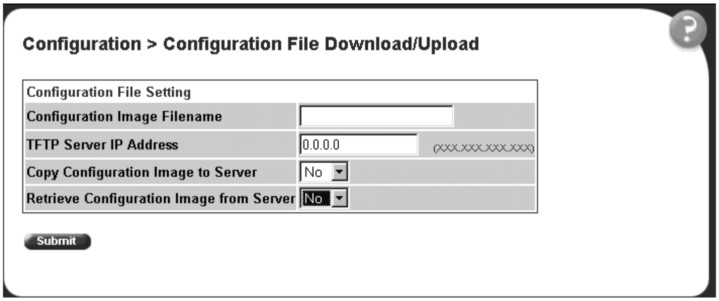
To download the BPS 2000 configuration file, a properly configured TFTP server must be present in your network, and the policy switch must have an IP address. To learn how to configure the switch or stack IP address, refer to "Configuring BootP, IP, and gateway settings" on page 58.

To store or retrieve a switch or stack configuration file:

1 From the main menu, choose Configuration > Configuration File.

The Configuration File Download/Upload page opens (Figure 43).

Figure 43 Configuration File Download/Upload page



Configuration > Configuration File Download/Upload

Configuration File Setting	
Configuration Image Filename	
TFTP Server IP Address	0.0.0.0 (XXX.XXX.XXX.XXX)
Copy Configuration Image to Server	No
Retrieve Configuration Image from Server	No

Table 37 describes the items on the Configuration File page.

Table 37 Configuration File page items

Item	Range	Description
Configuration Image Filename	1..32	Type the configuration file name.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of the TFTP load host.
Copy Configuration Image to Server	(1) Yes (2) No	Choose whether or not to copy the configuration image to the server.
Retrieve Configuration Image from Server	(1) Yes (2) No	Choose whether or not to retrieve the configuration image from a server. If you choose Yes, the download process begins immediately and, when completed, causes the switch or stack to reset with the new configuration parameters.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Table 38 describes the requirements for storing or retrieving configuration parameters on a TFTP server.

Table 38 Requirements for storing or retrieving configuration parameters on a TFTP server

Requirements
• The Configuration File feature can only be used to copy *standalone switch configuration parameters to other standalone switches* or to copy *stack configuration parameters to other stack configurations*. For example, you cannot duplicate the configuration parameters of a unit in a *stack* configuration and use it to configure a *standalone* switch.
• A configuration file obtained from a standalone switch can only be used to configure other standalone switches that have the same firmware revision and model type as the donor standalone switch.
• A configuration file obtained from a stack unit can only be used to configure other stacks that have the same number of switches, firmware version, model types, and physical IDs as the stack the donor stack unit resides in.
• Reconfigured stacks are configured according to the unit order number of the donor unit. For example, the configuration file parameters from a donor unit with physical ID *x* are used to reconfigure the unit with physical ID *x*.
• The configuration file also duplicates any settings that exist for any MDA that is installed in the donor switch. If you use the configuration file to configure another switch that has the same MDA model installed, the configuration file settings will also apply to and override the existing MDA settings.

Table 39 describes the parameters that are not saved to the configuration file.

Table 39 Parameters not saved to the configuration file

These parameters are not saved:	**Used in this screen:**	**See page:**
In-Band Stack IP Address	IP Configuration/Setup	58
In-Band Switch IP Address		
In-Band Subnet Mask		
Default Gateway		
Configuration Image Filename	Configuration File Download/Upload	108
TFTP Server IP Address		
Console Read-Only Switch Password	Console/Comm Port Configuration	111
Console Read-Write Switch Password		
Console Read-Only Stack Password		
Console Read-Write Stack Password		

Configuring port communication speed

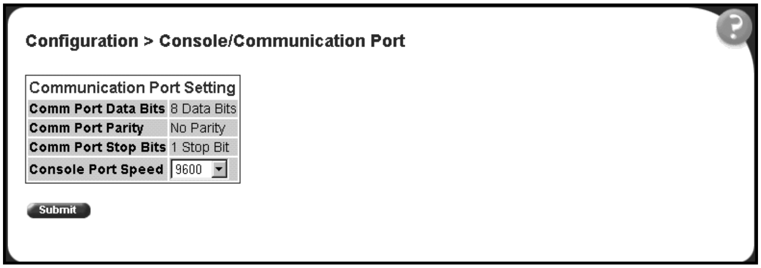
You can view the current console/communication port settings and configure the console port baud rate to match the baud rate of the console terminal.

To view current console/communication port settings and configure console port speed:

1 From the main menu, choose Configuration > Console/Comm Port.

The Console/Communication Port page opens (Figure 44).

Figure 44 Console/Communication Port page



Configuration > Console/Communication Port

Communication Port Setting	
Comm Port Data Bits	8 Data Bits
Comm Port Parity	No Parity
Comm Port Stop Bits	1 Stop Bit
Console Port Speed	9600

Table 40 describes the items on the Console/Communication Port page.

Table 40 Console/Communication Port Setting page items

Item	**Range**	**Description**
Comm Port Data Bits		The current console communication port data bit setting.
Comm Port Parity		The current console communication port parity setting.
Comm Port Stop Bits		The current console communication port stop bit setting.
Console Port Speed	2400 4800 9600 19200 38400	Choose the console port speed baud rate. Note: The default setting is 9600.
		Caution: If you choose a baud rate that does not match your console terminal baud rate, you will lose communication with the configuration interface when you click Submit.

2 Select from the list.

3 Click Submit.

Setting system operational modes

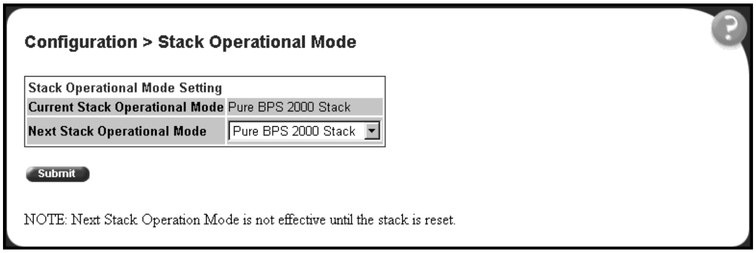
You can set the next stack mode operation of either a stack of BPS 2000es only, or a mixed stack of BPS 2000es and BayStack 450 and 410 switches.

To set the next stack mode operation:

1 From the main menu, choose Configuration > Stack Operational Mode.

The Stack Operational Mode Setting page opens (Figure 45).

Figure 45 Stack Operational Mode page



Configuration > Stack Operational Mode
Stack Operational Mode Setting
Submit

Current Stack Operational Mode: Pure BPS 2000 Stack
Next Stack Operational Mode: Pure BPS 2000 Stack

NOTE: Next Stack Operation Mode is not effective until the stack is reset.

Table 41 describes the items on the Stack Operational Mode Setting page.

Table 41 Stack Operational Mode page items

Item	Range	Description
Current Stack Operational Mode		Current stack operational mode. The options are Pure BPS 2000 Stack or Hybrid Stack.
Next Stack operational Mode	(1) Pure BPS 2000 Stack (2) Hybrid Stack	Choose whether your stack is BPS 2000es only, or a mixed stack of BayStack 450 and BPS 2000es (Hybrid Stack).

2 Select from the list.

3 Click Submit.

Chapter 5

Configuring remote network monitoring (RMON)

The RMON management information base (MIB) is an interface between the RMON agent on a BayStack 450 switch or Business Policy Switch 2000 and RMON management applications such as the Web-based management user interface. It defines objects that are suitable for the management of any type of network. Some groups are specifically targeted for Ethernet networks.

The RMON agent continuously collects statistics and proactively monitors the switch.

This RMON options available to you are:

- "Configuring RMON fault threshold parameters," (next)
- "Viewing the RMON fault event log" on page 117
- "Viewing the system log" on page 118
- "Viewing RMON Ethernet statistics" on page 120
- "Viewing RMON history" on page 124

Note: To access the software version 1.2 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Configuring RMON fault threshold parameters

Alarms are useful when you need to know when the value of some variable goes out of range. RMON alarms can be defined on any MIB variable that resolves to an integer value. String variables (such as system description) cannot be used as alarm variables.

Creating an RMON fault threshold

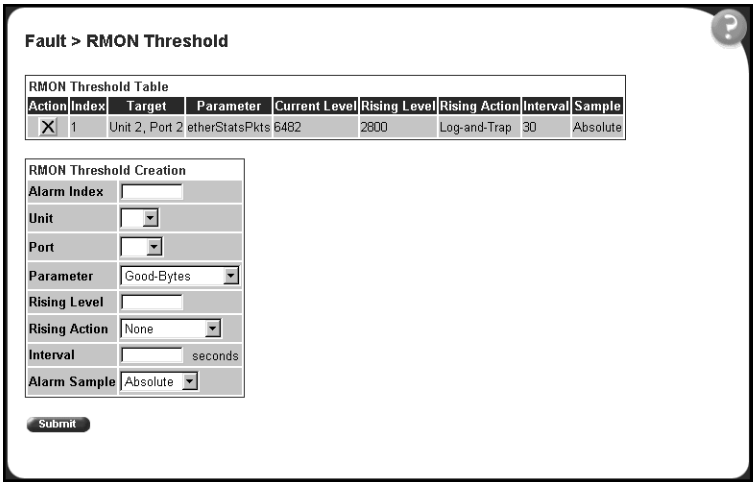
You can create the RMON threshold parameters for fault notification (alarms).

To create an RMON threshold:

1 From the main menu, choose Fault > RMON Threshold.

The RMON Threshold page opens (Figure 46).

Figure 46 RMON Threshold page



Fault > RMON Threshold

RMON Threshold Table

Action	Index	Target	Parameter	Current Level	Rising Level	Rising Action	Interval	Sample
☒	1	Unit 2, Port 2	etherStatsPkts	6482	2800	Log-and-Trap	30	Absolute

RMON Threshold Creation

Alarm Index	
Unit	
Port	
Parameter	Good-Bytes
Rising Level	
Rising Action	None
Interval	seconds
Alarm Sample	Absolute

Table 42 describes the items on the RMON Threshold page.

Table 42 RMON Threshold page items

Item	Range	Description
☒		Deletes the row.
Index/Alarm Index	1..10	Type the unique number to identify the alarm entry.
Target	Integer	The unit number and port number.
Unit	1..8	Choose the switch on which to configure port alarms.
Port	1..28	Choose the port on which to set an alarm.
Parameter	(1) Good-Bytes (2) Good-Packets (3) Multicast (4) Broadcast (5) CRC-Errors (6) Misaligned (7) Runts (8) Fragments (9) Frame-Too-Long (10) Collisions (11) Late Collisions	Choose the sampled statistic.
Current Level	Integer	The value of the statistic during the last sampling period. Note: If the sample type is Delta, the value is the difference between the samples at the *beginning and end* of the period. If the sample type is Absolute, the value is the sampled value at the *end* of the period.
Rising Level	Integer	Type the event entry to be used when a rising threshold is crossed. Note: When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the Falling Threshold.
Rising Action	(1) None (2) Log (3) SNMP-Trap (4) Log-and-Trap	Choose the type of notification for the event. Selecting Log generates an entry in the RMON Event Log table for each event. Selecting SNMP Trap sends an SNMP trap to one or more management stations.

Table 42 RMON Threshold page items (continued)

Item	Range	Description
Interval		Type the time period (in seconds) to sample data and compare the data to the rising and falling thresholds.
Sample/Alarm Sample	(1) Absolute (2) Delta	Choose the sampling method: Absolute: *Absolute* alarms are defined on the current value of the alarm variable. An example of an alarm defined with absolute value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you set it for absolute value. Therefore, an alarm could be created with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down. Delta: Most alarm variables related to Ethernet traffic are set to *delta* value. Delta alarms are defined based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice per polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision and allows for the detection of threshold crossings that span the sampling boundary. Therefore, if you keep track of the current values of a given delta-valued alarm and add them together, the result is twice the actual value. (This result is not an error in the software.)

2 In the RMON Threshold Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new configuration is displayed in the RMON Threshold Table (Figure 46).

➡ **Note:** RMON threshold configurations are not modifiable. They must be deleted and the information recreated.

Deleting an RMON threshold configuration

To delete an existing RMON threshold configuration:

1 From the main menu, choose Fault > RMON Threshold.

The RMON Threshold page opens (Figure 46).

2 In the RMON Threshold Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the RMON threshold configuration.
- Click Cancel to return to the RMON Threshold page without making changes.

Viewing the RMON fault event log

RMON events and alarms work together to notify you when values in your network go out of a specified range. When values pass the specified ranges, the alarm is triggered and “fires.” The event specifies how the activity is recorded.

An event specifies whether a trap, a log, or a trap and a log are generated to view alarm activity. When RMON is globally enabled, two default events are generated:

- Rising Event
- Falling Event

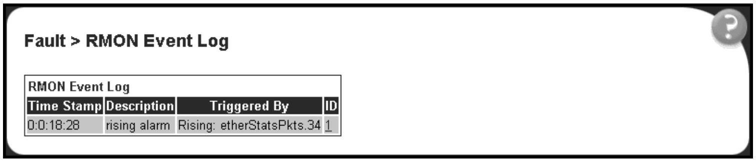
Default events specify that when an alarm goes out of range, the firing of the alarm is tracked in both a trap and a log. For example, when an alarm fires at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. The RMON Event Log page works in conjunction with the RMON Threshold page to enable you to view a history of RMON fault events.

To view a history of RMON fault events:

➨ From the main menu, choose Fault > RMON Event Log.

The RMON Event Log page opens (Figure 47).

Figure 47 RMON Event Log page



Fault > RMON Event Log

RMON Event Log

Time Stamp	Description	Triggered By	ID
0:0:18:28	rising alarm	Rising: etherStatsPkts.34	1

Table 43 describes the fields on the RMON Event Log page.

Table 43 RMON Event Log page fields

Item	Description
Time Stamp	The time the event occurred.
Description	An implementation dependent description of the event that activated this log entry.
Triggered By	A comment describing the source of the event.
ID	The event that generated this log entry.

Viewing the system log

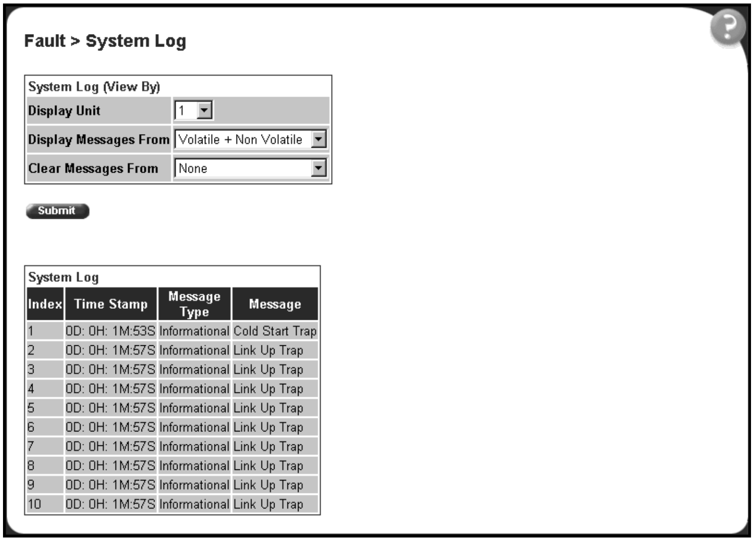
You can view a display of messages contained in non-volatile random access memory (NVRAM) or dynamic random access memory (DRAM) and NVRAM.

To open the System Log page:

1 From the main menu, choose Fault > System Log.

The System Log page opens (Figure 48).

Figure 48 System Log page



System Log (View By)

Display Unit	1
Display Messages From	Volatile + Non Volatile
Clear Messages From	None

System Log

Index	Time Stamp	Message Type	Message
1	0D: 0H: 1M:53S	Informational	Cold Start Trap
2	0D: 0H: 1M:57S	Informational	Link Up Trap
3	0D: 0H: 1M:57S	Informational	Link Up Trap
4	0D: 0H: 1M:57S	Informational	Link Up Trap
5	0D: 0H: 1M:57S	Informational	Link Up Trap
6	0D: 0H: 1M:57S	Informational	Link Up Trap
7	0D: 0H: 1M:57S	Informational	Link Up Trap
8	0D: 0H: 1M:57S	Informational	Link Up Trap
9	0D: 0H: 1M:57S	Informational	Link Up Trap
10	0D: 0H: 1M:57S	Informational	Link Up Trap

Table 44 describes the fields on the System Log page.

Table 44 System Log page fields

Section	Item	Range	Description
System Log (View By)	Display Unit	1..8	Choose the unit on which to display messages or clear messages.
	Display Messages From	(1) Non Volatile (2) Volatile + Non Volatile	Choose to display messages from Non Volatile memory (NVRAM) or Volatile (DRAM) and Non Volatile memory. The default settings is Non Volatile.
	Clear Messages From	(1) Volatile (2) Volatile + Non Volatile (3) None	Choose to clear messages from Volatile memory or Volatile and Non Volatile memory. The default settings is None (do not clear messages)
System Log	Index		The number of the event.
	Time Stamp		The time, in hundreths of a second, between system initialization and the time the log messages entered the system.
	Message Type		The type of message. The options are (1) Critical, (2) Serious, and (3) Informational.
	Message		A character string that identifies the origin of the message and the reason why the message was generated.

2 In the System Log (View By) section do one or more of the following:

- Choose the number of the unit from which to display messages.
- Choose where to display messages from.
- Choose to clear messages from Volatile or Non Volatile memory.

3 Click Submit.

The results of your request are displayed in the System Log section (Figure 48).

Viewing RMON Ethernet statistics

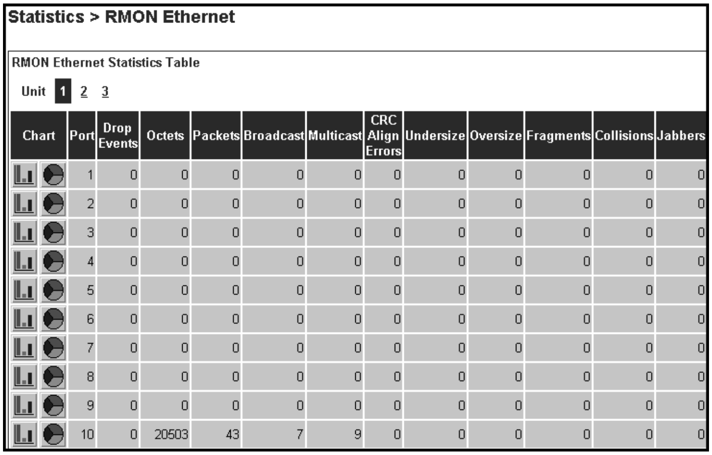
You can gather and graph RMON Ethernet statistics in a variety of formats.

To gather and graph RMON Ethernet statistics:

1. From the main menu, choose Statistics > RMON Ethernet.

   The RMON Ethernet page opens (Figure 49).

Figure 49 RMON Ethernet page



Statistics > RMON Ethernet

RMON Ethernet Statistics Table

Unit **1** 2 3

Chart	Port	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors	Undersize	Oversize	Fragments	Collisions	Jabbers
📊 ◕	1	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	2	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	3	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	4	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	5	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	6	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	7	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	8	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	9	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	10	0	20503	43	7	9	0	0	0	0	0	0

Table 45 describes the items on the RMON Ethernet page.

Table 45 RMON Ethernet page items

Item	Description
📊	Displays statistics as a bar graph.
◕	Displays statistics as a pie chart.
Port	The port number that corresponds to the selected switch.
Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).

Table 45 RMON Ethernet page items (continued)

Item	Description
Packets	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
Broadcast	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
Multicast	The number of good packets received that were directed to the multicast address. This *does not* include packets sent to the broadcast address.
CRC Align Errors	The number of packets received that had a length (excluding and 1518 octets, inclusive, but had either a bad Frame FCS with an integral number of octets (FCS errors) with a non-integral number of octets (alignment error).
Undersize	The number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Oversize	The number of packets received that were longer than 1518 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Fragments	The number of packets received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The “best estimate” number of collisions on this Ethernet segment.
Jabbers	The number of packets received that were longer than 1518 octets in length (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Packets < = 64 bytes 65-127 bytes 128-255 bytes 256-511 bytes 512-1023 bytes 1024-1518 bytes	The number of octets received (including bad packets) in length (excluding framing bits, but including FCS octets).

2 In the upper-left hand corner, click on the unit number of the device to monitor.

3 Click Submit.

The RMON Ethernet Statistics Table is updated with information about the selected device (Figure 49).

Viewing RMON Ethernet statistics in a bar graph format

To view RMON Ethernet statistics in a bar graph format:

1 From the main menu, choose Statistics > RMON Ethernet.

The RMON Ethernet page opens (Figure 49).

2 In the port row of your choice, click the bar graph icon.

The RMON Ethernet: Chart page appears in a bar graph format (Figure 50).

Figure 50 RMON Ethernet: Chart in a bar graph format

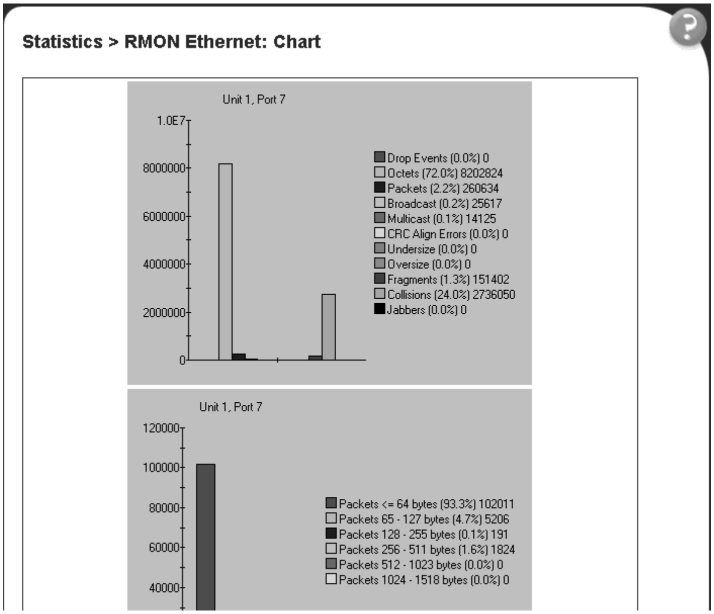

Statistics > RMON Ethernet: Chart
Unit 1, Port 7
1.0E7
8000000
6000000
4000000
2000000
0
Drop Events (0.0%) 0
Octets (72.0%) 8202824
Packets (2.2%) 260634
Broadcast (0.2%) 25617
Multicast (0.1%) 14125
CRC Align Errors (0.0%) 0
Undersize (0.0%) 0
Oversize (0.0%) 0
Fragments (1.3%) 151402
Collisions (24.0%) 2736050
Jabbers (0.0%) 0
Unit 1, Port 7
120000
100000
80000
60000
40000
Packets <= 64 bytes (93.3%) 102011
Packets 65 - 127 bytes (4.7%) 5206
Packets 128 - 255 bytes (0.1%) 191
Packets 256 - 511 bytes (1.6%) 1824
Packets 512 - 1023 bytes (0.0%) 0
Packets 1024 - 1518 bytes (0.0%) 0

Table 45 describes the items on the RMON Ethernet: Chart page.

3 To refresh statistical information, go to the bottom of the page and click Update, or click Back to return to the Ethernet Statistics page.

Viewing RMON Ethernet statistics in a pie chart format

To view RMON Ethernet statistics in a pie chart format:

1. From the main menu, choose Statistics > RMON Ethernet.

   The RMON Ethernet page opens (Figure 49).

2. In the port row of your choice, click the pie chart icon.

   The RMON Ethernet: Chart page appears in a pie chart format (Figure 51).

Figure 51 RMON Ethernet: Chart in a pie chart format

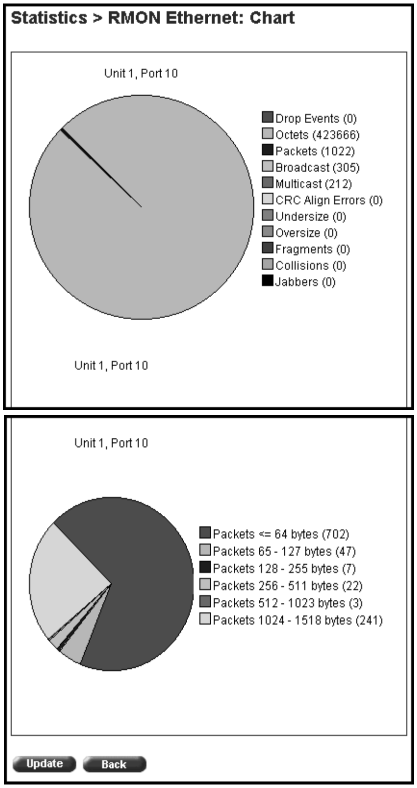

Statistics > RMON Ethernet: Chart
Unit 1, Port 10
Drop Events (0)
Octets (423666)
Packets (1022)
Broadcast (305)
Multicast (212)
CRC Align Errors (0)
Undersize (0)
Oversize (0)
Fragments (0)
Collisions (0)
Jabbers (0)
Unit 1, Port 10
Unit 1, Port 10
Packets <= 64 bytes (702)
Packets 65 - 127 bytes (47)
Packets 128 - 255 bytes (7)
Packets 256 - 511 bytes (22)
Packets 512 - 1023 bytes (3)
Packets 1024 - 1518 bytes (241)
Update
Back

Table 45 describes the items on the RMON Ethernet: Chart page.

3. To refresh statistical information, click Update, or click Back to return to the Ethernet Statistics page.

Viewing RMON history

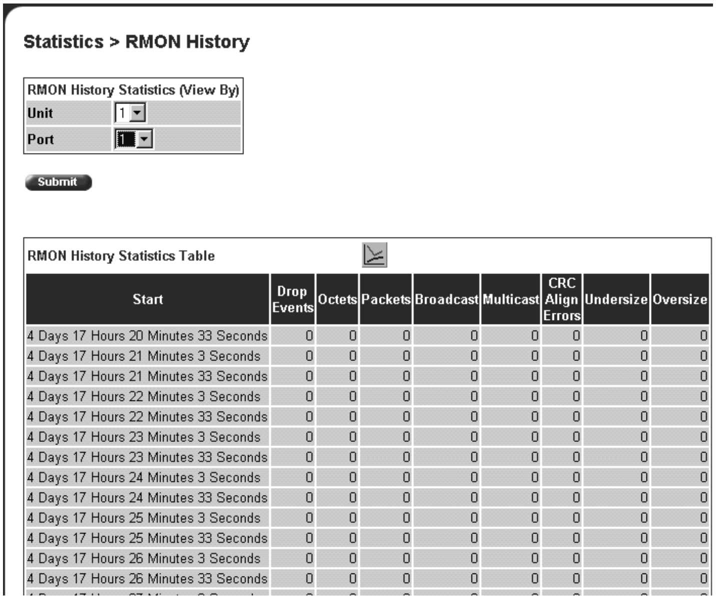
You can view a periodic statistical sampling of data from various types of networks.

To view periodic statistical data:

1 From the main menu, choose Statistics > RMON History.

The RMON History page opens (Figure 52).

Figure 52 RMON History page



Statistics > RMON History

RMON History Statistics (View By)	
Unit	1
Port	1

RMON History Statistics Table

Start	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors	Undersize	Oversize
4 Days 17 Hours 20 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 21 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 21 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 22 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 22 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 23 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 23 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 24 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 24 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 25 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 25 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 26 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 26 Minutes 33 Seconds	0	0	0	0	0	0	0	0

Table 46 describes the items on the RMON History page.

Table 46 RMON History page items

Section	Item	Description
RMON History Statistics (View By)	Unit	Choose the unit number to be monitored.
	Port	Choose the port number to be monitored.
	📈	Displays statistics as a line graph.
RMON History Statistics Table	Start	The value of the sysUPTime at the start of the interval over which this sample was measured.
	Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
	Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).
	Packets	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
	Broadcast	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
	Multicast	The number of good packets received that were directed to the multicast address. This *does not* include packets sent to the broadcast address.
	CRC Align Errors	The number of packets received that had a length (excluding and 1518 octets, inclusive, but had either a bad Frame FCS with an integral number of octets (FCS errors) with a non-integral number of octets (alignment error).
	Undersize	The number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
	Oversize	The number of packets received that were longer than 1518 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.

2 In the RMON History Statistics section, choose the unit and port number to be monitored.

3 Click Submit.

The RMON History Statistics Table is updated with information about the selected device and port (Figure 52).

Viewing RMON statistics in a line graph format

You can view RMON statistical data in a line graph format.

To view statistics in a line graph format:

1. From the main menu, choose Statistics > RMON History.

   The RMON History page opens (Figure 52).

2. In the RMON History Statistics Table, click the line graph icon.
3. Click Back to return to the RMON History page.

Chapter 6
Viewing system statistics

The options available to monitor system statistical data are:

- "Viewing port statistics," (next)
- "Viewing all port errors" on page 132
- "Viewing interface statistics" on page 134
- "Viewing Ethernet error statistics" on page 137
- "Viewing transparent bridging statistics" on page 141

Note: To access the software version 1.2 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Viewing port statistics

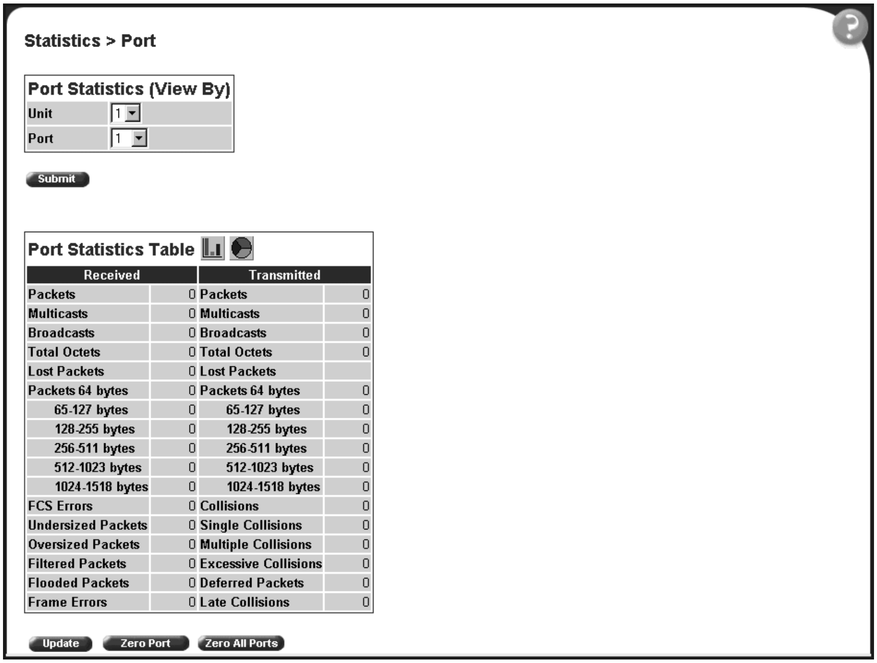
You can view detailed statistics about a selected switch port in a stacked or standalone configuration. Both received and transmitted statistics are displayed so that you can compare throughput or other port parameters.

To view statistical data about a selected switch port:

1 From the main menu, choose Statistics > Port.

The Port page opens (Figure 53).

Figure 53 Port page



Statistics > Port

Port Statistics (View By)	
Unit	1
Port	1

Port Statistics Table

Received		Transmitted	
Packets	0	Packets	0
Multicasts	0	Multicasts	0
Broadcasts	0	Broadcasts	0
Total Octets	0	Total Octets	0
Lost Packets	0	Lost Packets	
Packets 64 bytes	0	Packets 64 bytes	0
65-127 bytes	0	65-127 bytes	0
128-255 bytes	0	128-255 bytes	0
256-511 bytes	0	256-511 bytes	0
512-1023 bytes	0	512-1023 bytes	0
1024-1518 bytes	0	1024-1518 bytes	0
FCS Errors	0	Collisions	0
Undersized Packets	0	Single Collisions	0
Oversized Packets	0	Multiple Collisions	0
Filtered Packets	0	Excessive Collisions	0
Flooded Packets	0	Deferred Packets	0
Frame Errors	0	Late Collisions	0

Table 47 describes the items on the Port page.

Table 47 Port page items

Section	Item	Description
Port Statistics (View By)	Unit	Choose the number of the switch to monitor.
	Port	Choose the switch's port number to monitor.
	📊	Displays statistics in a bar graph format.
	◕	Displays statistics in a pie chart format.

Table 47 Port page items (continued)

Section	**Item**	**Description**
Port Statistics Table	Packets	The number of packets received/transmitted on this port, including bad packets, broadcast packets, and multicast packets.
	Multicast	The number of good multicast packets received/transmitted on this port, excluding broadcast packets.
	Broadcasts	The number of good broadcast packets received/transmitted on this port.
	Total Octets	The number of octets of data received/transmitted on this port, including data in bad packets and FCS octets, and framing bits.
	Lost Packets	The number of packets discarded on this port when the capacity of the port transmit buffer was exceeded.
	Packets = 64 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 65-127 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 128-255 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 256-511 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 512-1023 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 1024-1518 bytes	The number of packets this size received/transmitted successfully on this port.
	FCS Errors	The number of valid-size packets received on this port with proper framing but discarded because of cyclic redundancy check (CRC) errors.
	Undersized Packets	The number of packets received on this port with fewer than 64 bytes and with proper CRC and framing (also known as short frames or runts).
	Oversized Packets	The number of packets that were received on this port with proper CRC and framing that meet the following requirements: • 1518 bytes if no VLAN tag exists • 1522 bytes if a VLAN tag exists
	Filtered Packets	The number of packets filtered, but not forwarded on this port.
	Flooded Packets	The number of packets flooded (forwarded) through this port because the destination address was not recognized in the address database.
	Frame Errors	The number of valid-size packets received on this port but discarded because of CRC errors and improper framing.

Table 47 Port page items (continued)

Section	Item	Description
Port Statistics Table, cont.	Collisions	The number of collisions detected on this port.
	Single Collisions	The number of packets that were transmitted successfully on this port after a single collision.
	Multiple Collisions	The number of packets that were transmitted successfully on this port after more than one collision.
	Excessive Collisions	The number of packets lost on this port due to excessive collisions.
	Deferred Packets	The number of frames that were delayed on the first transmission attempt, but never incurred a collision.
	Late Collisions	The number of packets collisions that occurred after a total length of time that exceeded 512 bit-times of packet transmission.

2 In the Port Statistics section, choose the unit number and its port number.

3 Click Submit.

The Port Statistics Table is updated with information about the selected device and port (Figure 53).

4 To update the statistical information, click Update.

Zeroing ports

To clear the statistical information for the currently displayed port:

➨ Click Zero Port.

To clear the statistical information for all ports in a switch or stack configuration:

➨ Click Zero All Ports.

Viewing port statistics in a pie chart format

You can view port statistics in a pie chart format.

To view the displayed statistical information in a pie chart format:

1 In the Port Statistics Table, click the pie chart icon.

The Port: Chart page opens in a pie chart format (Figure 54).

Figure 54 Port: Chart page in a pie chart format

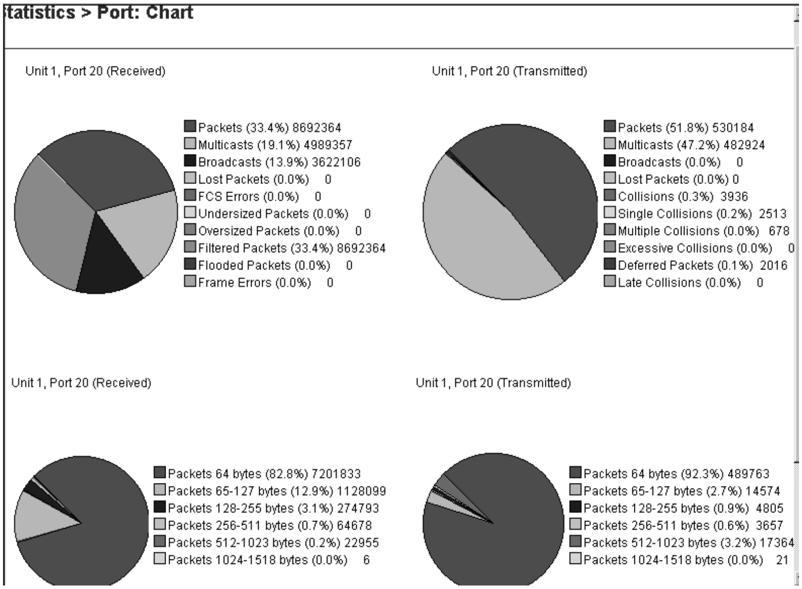

tatistics > Port: Chart
Unit 1, Port 20 (Received)
Packets (33.4%) 8692364
Multicasts (19.1%) 4989357
Broadcasts (13.9%) 3622106
Lost Packets (0.0%) 0
FCS Errors (0.0%) 0
Undersized Packets (0.0%) 0
Oversized Packets (0.0%) 0
Filtered Packets (33.4%) 8692364
Flooded Packets (0.0%) 0
Frame Errors (0.0%) 0
Unit 1, Port 20 (Transmitted)
Packets (51.8%) 530184
Multicasts (47.2%) 482924
Broadcasts (0.0%) 0
Lost Packets (0.0%) 0
Collisions (0.3%) 3936
Single Collisions (0.2%) 2513
Multiple Collisions (0.0%) 678
Excessive Collisions (0.0%) 0
Deferred Packets (0.1%) 2016
Late Collisions (0.0%) 0
Unit 1, Port 20 (Received)
Packets 64 bytes (82.8%) 7201833
Packets 65-127 bytes (12.9%) 1128099
Packets 128-255 bytes (3.1%) 274793
Packets 256-511 bytes (0.7%) 64678
Packets 512-1023 bytes (0.2%) 22955
Packets 1024-1518 bytes (0.0%) 6
Unit 1, Port 20 (Transmitted)
Packets 64 bytes (92.3%) 489763
Packets 65-127 bytes (2.7%) 14574
Packets 128-255 bytes (0.9%) 4805
Packets 256-511 bytes (0.6%) 3657
Packets 512-1023 bytes (3.2%) 17364
Packets 1024-1518 bytes (0.0%) 21

Table 47 describes the items on the Port: Chart page.

2 Click Back to return to the Port page.

Viewing port statistics in a bar graph format

You can view port statistics in a bar graph format.

To view the displayed statistical information in a bar graph format:

1 In the Port Statistics Table, click the bar graph icon.

The Port: Chart page opens in a bar graph format (Figure 55).

Figure 55 Port: Chart page in a bar graph format

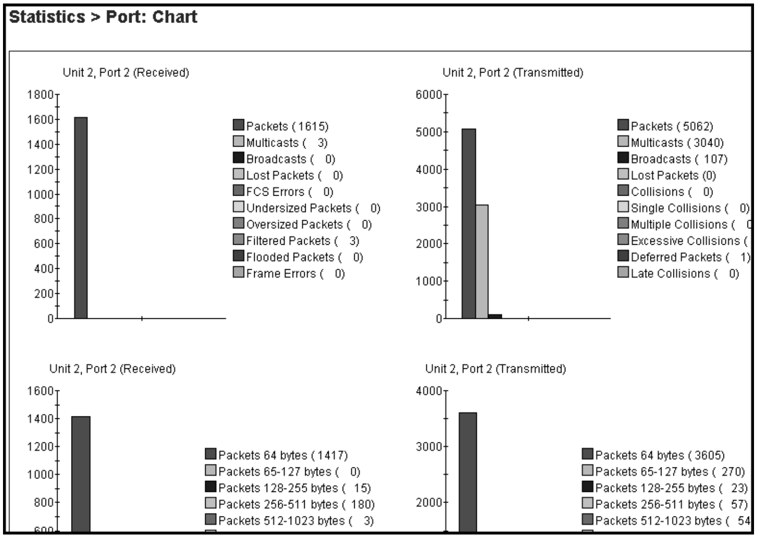

Statistics > Port: Chart
Unit 2, Port 2 (Received)
1800
1600
1400
1200
1000
800
600
400
200
0
■ Packets (1615)
□ Multicasts (3)
■ Broadcasts (0)
□ Lost Packets (0)
■ FCS Errors (0)
□ Undersized Packets (0)
■ Oversized Packets (0)
■ Filtered Packets (3)
■ Flooded Packets (0)
□ Frame Errors (0)
Unit 2, Port 2 (Transmitted)
6000
5000
4000
3000
2000
1000
0
■ Packets (5062)
□ Multicasts (3040)
■ Broadcasts (107)
□ Lost Packets (0)
■ Collisions (0)
□ Single Collisions (0)
■ Multiple Collisions (
■ Excessive Collisions (
■ Deferred Packets (1)
□ Late Collisions (0)
Unit 2, Port 2 (Received)
1600
1400
1200
1000
800
600
■ Packets 64 bytes (1417)
□ Packets 65-127 bytes (0)
■ Packets 128-255 bytes (15)
□ Packets 256-511 bytes (180)
■ Packets 512-1023 bytes (3)
Unit 2, Port 2 (Transmitted)
4000
3000
2000
■ Packets 64 bytes (3605)
□ Packets 65-127 bytes (270)
■ Packets 128-255 bytes (23)
□ Packets 256-511 bytes (57)
■ Packets 512-1023 bytes (54

Table 47 describes the items on the Port: Chart page.

2 Click Back to return to the Port page.

Viewing all port errors

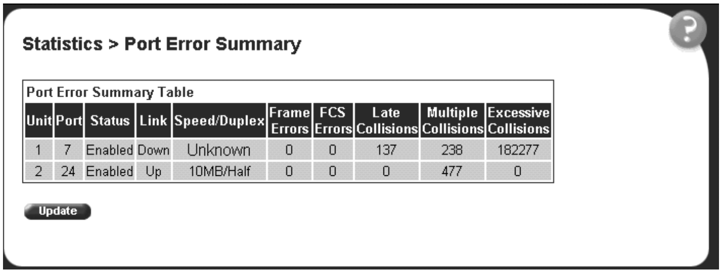
Beginning with software version 1.1, you can view all ports in the entire stack that have an error. If a particular port has no errors, it will not be displayed.

To view a summary of the port errors for the BPS 2000:

1 From the main menu, choose Statistics > Port Error Summary.

The Port Error Summary page opens (Figure 56).

Figure 56 Port Error Summary page



Statistics > Port Error Summary

Port Error Summary Table

Unit	Port	Status	Link	Speed/Duplex	Frame Errors	FCS Errors	Late Collisions	Multiple Collisions	Excessive Collisions
1	7	Enabled	Down	Unknown	0	0	137	238	182277
2	24	Enabled	Up	10MB/Half	0	0	0	477	0

Table 48 describes the read-only information displayed in the Port Error Summary Table.

Table 48 Port Error Summary Table fields

Item	Description
Unit	Displays the unit number in the stack.
Port	Displays the port number of the unit.
Status	Displays the status of the port (Enabled/Disabled).
Link	Displays the link status of the port (Up/Down).
Speed/Duplex	Displays the speed at which the port is operating, as well as whether it is in half- or full-duplex mode.
Frame Errors	Displays the number of frame errors received on this port.
FCS Errors	Displays the number of frame check sequence (FCS) errors received on this port.
Late Collisions	Displays the number of late collisions errors received on this port.
Multiple Collisions	Displays the number of multiple collisions errors received on this port.
Excessive Collisions	Displays the number of excessive collisions errors received on this port.

2 To view the latest port statistics, click the Update button at the bottom of the page.

Viewing interface statistics

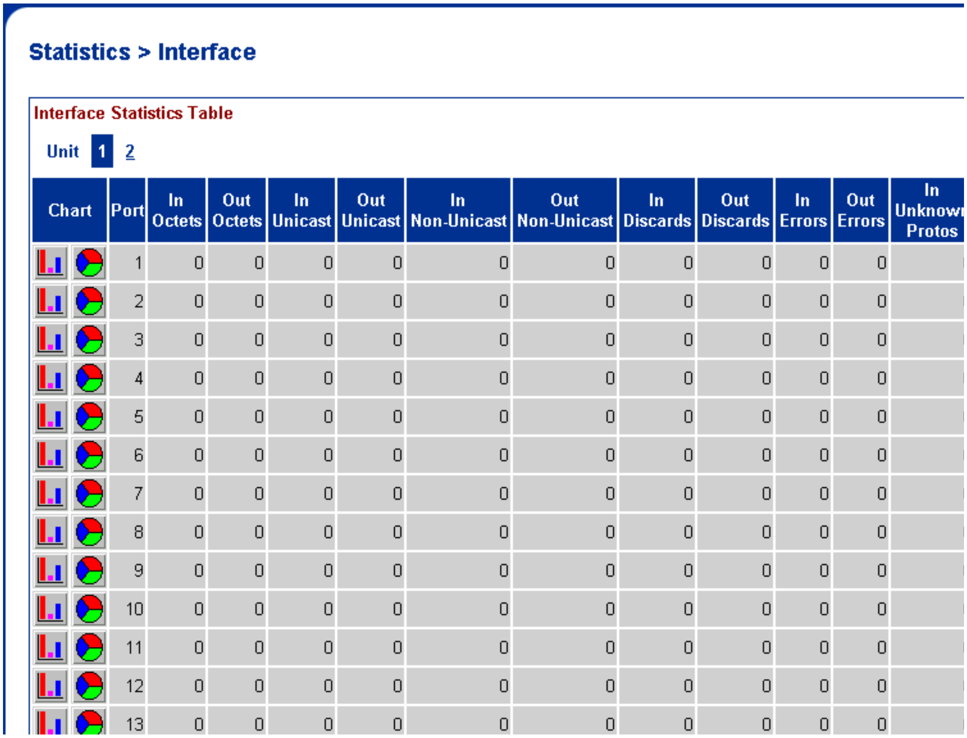
You can view selected switch interface statistics.

To view an interface's statistical information:

1 From the main menu, choose Statistics > Interface.

The Interface page opens (Figure 57).

Figure 57 Interface page



Statistics > Interface

Interface Statistics Table

Unit **1** 2

Chart	Port	In Octets	Out Octets	In Unicast	Out Unicast	In Non-Unicast	Out Non-Unicast	In Discards	Out Discards	In Errors	Out Errors	In Unknow Protos
📊 ◕	1	0	0	0	0	0	0	0	0	0	0	
📊 ◕	2	0	0	0	0	0	0	0	0	0	0	
📊 ◕	3	0	0	0	0	0	0	0	0	0	0	
📊 ◕	4	0	0	0	0	0	0	0	0	0	0	
📊 ◕	5	0	0	0	0	0	0	0	0	0	0	
📊 ◕	6	0	0	0	0	0	0	0	0	0	0	
📊 ◕	7	0	0	0	0	0	0	0	0	0	0	
📊 ◕	8	0	0	0	0	0	0	0	0	0	0	
📊 ◕	9	0	0	0	0	0	0	0	0	0	0	
📊 ◕	10	0	0	0	0	0	0	0	0	0	0	
📊 ◕	11	0	0	0	0	0	0	0	0	0	0	
📊 ◕	12	0	0	0	0	0	0	0	0	0	0	
📊 ◕	13	0	0	0	0	0	0	0	0	0	0	

Table 49 describes the items on the Interface page.

Table 49 Interface page items

Item	Description
📊	Displays statistics in a bar graph format.
◕	Displays statistics in a pie chart format.
Port	The port number corresponding to the selected switch.
In Octets	The number of octets received on the interface, including framing characters.
Out Octets	The number of octets transmitted out of the interface, including framing characters.
In Unicast	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Out Unicast	The number of packets that higher-layer protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
In Non-Unicast	The number of non-unicast packets, for example, subnetwork-broadcast or subnetwork-multicast packets, delivered to a higher protocol.
Out Non-Unicast	The number of packets that higher-level protocols requested be transmitted to a non-unicast address. For example, a subnetwork-broadcast or a subnetwork multicast address, including those that were discarded or not sent.
In Discards	The number of inbound packets which were selected to be discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
Out Discards	The number of outbound packets which were selected to be discarded even though no errors were detected to prevent their being transmitted. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
In Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Out Errors	The number of outbound packets that could not be transmitted because of errors.
In Unknown Protos	The number of packets received through the interface that were discarded because of an unknown or unsupported protocol.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

The page is updated with the information for the selected device (Figure 57).

3 To update the statistical information, click Update.

Viewing interface statistics in a pie chart format

You can view interface statistics in a pie chart format.

To view interface statistics in a pie chart format:

1 From the main menu, choose Statistics > Interface.

The Interface page opens (Figure 57).

2 In the port row of your choice, click the pie chart icon.

The Interface: Chart page opens in a pie chart format (Figure 58).

Figure 58 Interface: Chart in a pie chart format

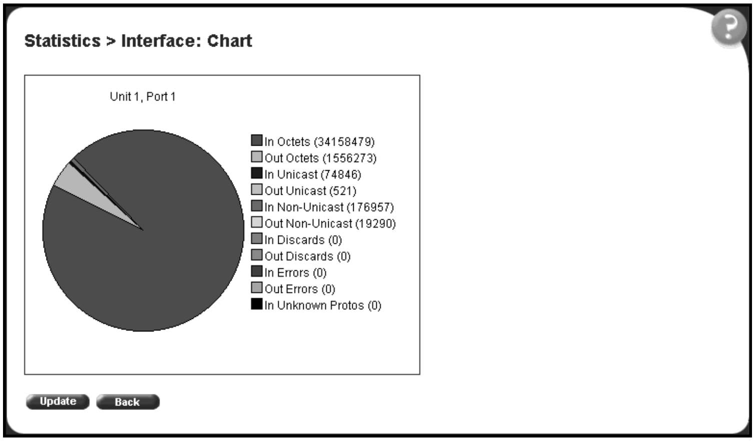

Statistics > Interface: Chart
Unit 1, Port 1
In Octets (34158479)
Out Octets (1556273)
In Unicast (74846)
Out Unicast (521)
In Non-Unicast (176957)
Out Non-Unicast (19290)
In Discards (0)
Out Discards (0)
In Errors (0)
Out Errors (0)
In Unknown Protos (0)
Update
Back

Table 49 describes the items on the Interface: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Interface page.

Viewing interface statistics in a bar graph format

You can view interface statistics in a bar graph format.

To view interface statistics in a bar graph format:

1 From the main menu, choose Statistics > Interface.

The Interface page opens (Figure 57).

2 In the port row of your choice, click the bar graph icon.

The Interface: Chart page opens in a bar graph format (Figure 58).

Figure 59 Interface: Chart in a bar graph format

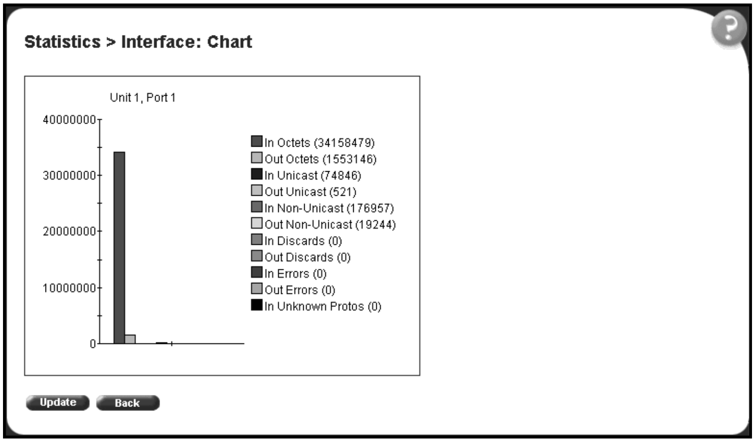

Statistics > Interface: Chart
Unit 1, Port 1
40000000
30000000
20000000
10000000
0
▩ In Octets (34158479)
☐ Out Octets (1553146)
■ In Unicast (74846)
☐ Out Unicast (521)
▩ In Non-Unicast (176957)
☐ Out Non-Unicast (19244)
▩ In Discards (0)
▩ Out Discards (0)
▩ In Errors (0)
▩ Out Errors (0)
■ In Unknown Protos (0)
Update
Back

Table 49 describes the items on the Interface: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Interface page.

Viewing Ethernet error statistics

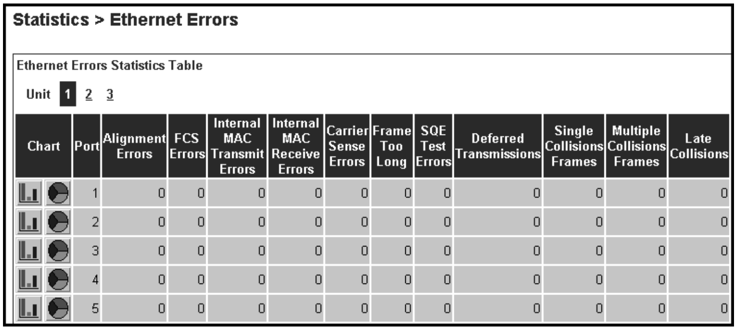
You can view Ethernet error statistics for each monitored interface linked to the Business Policy Switch 2000.

To view Ethernet error statistics:

1 From the main menu, choose Statistics > Ethernet Errors.

The Ethernet Errors page opens (Figure 60).

Figure 60 Ethernet Errors page



Statistics > Ethernet Errors

Ethernet Errors Statistics Table

Unit **1** 2 3

Chart	Port	Alignment Errors	FCS Errors	Internal MAC Transmit Errors	Internal MAC Receive Errors	Carrier Sense Errors	Frame Too Long	SQE Test Errors	Deferred Transmissions	Single Collisions Frames	Multiple Collisions Frames	Late Collisions
📊 ◕	1	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	2	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	3	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	4	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	5	0	0	0	0	0	0	0	0	0	0	0

Table 50 describes the items on the Ethernet Errors page.

Table 50 Ethernet Errors page items

Item	Description
📊	Displays statistics in a bar graph format.
◕	Displays statistics in a pie chart format.
Port	The port number corresponding to the selected switch.
Alignment Errors	The number of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	The number of frames received on a particular interface that are an integral number of octets in length, but do not pass the FCS check.
Internal MAC Transmit Errors	The number of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
Internal MAC Receive Errors	The number of frames for which reception on a particular interface fails due to an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
Carrier Sense Errors	The number of times that the carrier sense conditions was lost or never asserted when attempting to transmit a frame on a particular interface.
Frame Too Long	The number of frames received on a particular interface that exceed the maximum permitted frame size.

Table 50 Ethernet Errors page items (continued)

Item	**Description**
SQE Test Errors	The number of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985, and its generation is described in section 7.2.4.6 of the same document.
Deferred Transmissions	The number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
Single Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Multiple Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by a single collision.
Late Collisions	The number of times a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
Excessive Collisions	The number of frames for which transmission on a particular interface fails due to excessive collisions.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

The table is updated with the information for the selected device.

3 To refresh the statistical information, click Update.

Viewing Ethernet error statistics in a pie chart format

You can view Ethernet Errors statistics in a pie chart format.

To view Ethernet Errors statistics in a pie chart format:

1 From the main menu, choose Statistics > Ethernet Errors.

The Ethernet Errors page opens (Figure 57).

2 In the port row of your choice, click the pie chart icon.

The Ethernet Errors: Chart page opens in a pie chart format (Figure 61).

Figure 61 Ethernet Error: Chart in a pie chart format

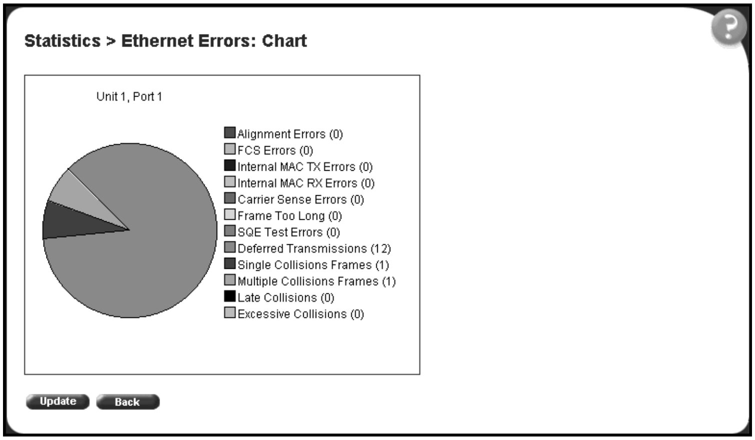

Statistics > Ethernet Errors: Chart
Unit 1, Port 1
Alignment Errors (0)
FCS Errors (0)
Internal MAC TX Errors (0)
Internal MAC RX Errors (0)
Carrier Sense Errors (0)
Frame Too Long (0)
SQE Test Errors (0)
Deferred Transmissions (12)
Single Collisions Frames (1)
Multiple Collisions Frames (1)
Late Collisions (0)
Excessive Collisions (0)
Update
Back

Table 51 describes the items on the Ethernet Errors: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Ethernet Errors page.

Viewing Ethernet error statistics in a bar graph format

You can view Ethernet Errors statistics in a bar graph format.

To view Ethernet errors statistics in a bar graph format:

1 From the main menu, choose Statistics > Ethernet Errors.

The Ethernet Errors page opens (Figure 57).

2 In the port row of your choice, click the bar graph icon.

The Ethernet Errors: Chart page opens in a bar graph format (Figure 62).

Figure 62 Ethernet Error: Chart in a bar graph format

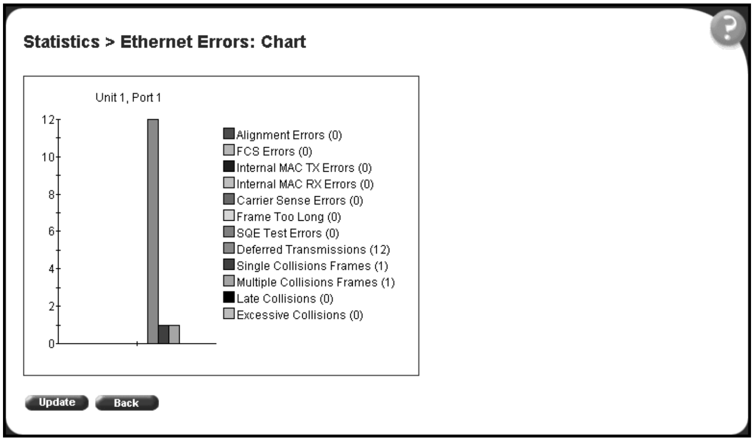

Statistics > Ethernet Errors: Chart
Unit 1, Port 1
12
10
8
6
4
2
0
Alignment Errors (0)
FCS Errors (0)
Internal MAC TX Errors (0)
Internal MAC RX Errors (0)
Carrier Sense Errors (0)
Frame Too Long (0)
SQE Test Errors (0)
Deferred Transmissions (12)
Single Collisions Frames (1)
Multiple Collisions Frames (1)
Late Collisions (0)
Excessive Collisions (0)
Update
Back

Table 50 describes the items on the Ethernet Errors: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Ethernet Errors page.

Viewing transparent bridging statistics

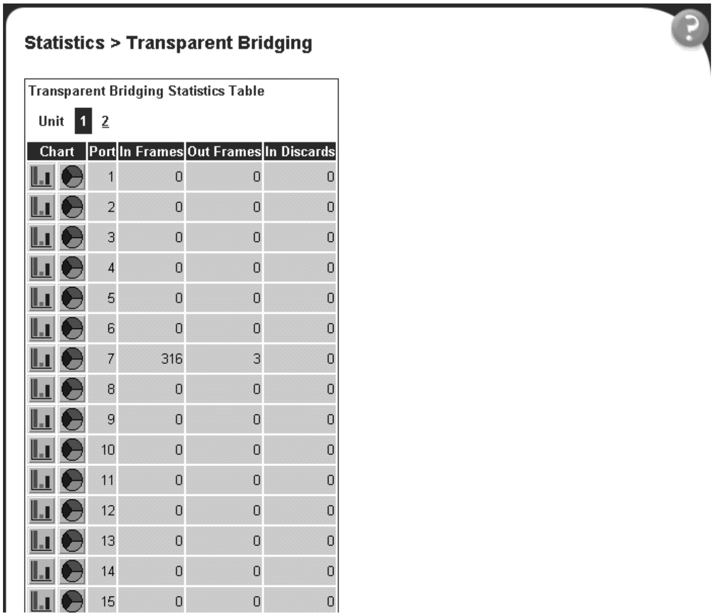
You can view the transparent bridging statistics measured for each monitored interface on the device.

To view transparent bridging statistics:

1 From the main menu, choose Statistics > Transparent Bridging.

The Transparent Bridging page opens (Figure 63).

Figure 63 Transparent Bridging page



Statistics > Transparent Bridging

Transparent Bridging Statistics Table

Unit **1** 2

Chart	Port	In Frames	Out Frames	In Discards
📊 ◔	1	0	0	0
📊 ◔	2	0	0	0
📊 ◔	3	0	0	0
📊 ◔	4	0	0	0
📊 ◔	5	0	0	0
📊 ◔	6	0	0	0
📊 ◔	7	316	3	0
📊 ◔	8	0	0	0
📊 ◔	9	0	0	0
📊 ◔	10	0	0	0
📊 ◔	11	0	0	0
📊 ◔	12	0	0	0
📊 ◔	13	0	0	0
📊 ◔	14	0	0	0
📊 ◔	15	0	0	0

Table 51 describes the items on the Transparent Bridging page.

Table 51 Transparent Bridging page items

Item	Description
📊	Displays statistics in a bar graph format.
◔	Displays statistics in a pie chart format.
Port	The port number that corresponds to the selected switch.
In Frames (dot1dTpPortInFrames)	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
Out Frames (dot1dTpPortOutFrames)	The number of frames that have been transmitted by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
In Discards (dot1dTpPortInDiscards)	The number of valid frames received which were discarded by the forwarding process.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

The page is updated with statistics about the selected device and its corresponding port number.

3 To refresh the statistical information, click Update.

Viewing transparent bridging statistics in a pie chart format

You can view measured transparent bridging statistics in a pie chart format.

To view transparent bridging statistics in a pie chart format:

1 From the main menu, choose Statistics > Transparent Bridging.

The Transparent Bridging page opens (Figure 57).

2 In the port row of your choice, click the pie chart icon.

The Transparent Bridging: Chart page opens in a pie chart format (Figure 64).

Figure 64 Transparent Bridging: Chart in a pie chart format

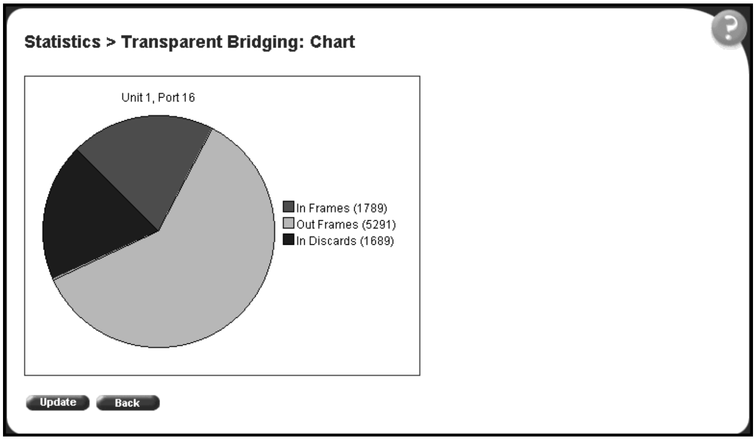


Table 51 describes the items on the Transparent Bridging: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Transparent Bridging page.

Viewing transparent bridging statistics in a bar graph format

You can view measured transparent bridging statistics in a bar graph format.

To view transparent bridging statistics in a bar graph format:

1. From the main menu, choose Statistics > Transparent Bridging.

   The Transparent Bridging page opens (Figure 57).

2. In the port row of your choice, click the bar graph icon.

   The Transparent Bridging: Chart page opens in a bar graph format (Figure 65).

Figure 65 Transparent Bridging: Chart in a bar graph format

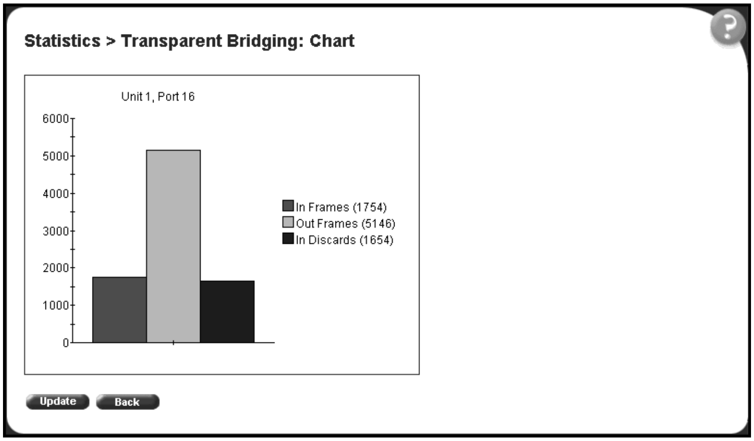

Statistics > Transparent Bridging: Chart
Unit 1, Port 16
6000
5000
4000
3000
2000
1000
0
In Frames (1754)
Out Frames (5146)
In Discards (1654)
Update
Back

   Table 51 describes the items on the Transparent Bridging: Chart page.

3. To update the statistical information, click Update, or click Back to return to the Transparent Bridging page.

Chapter 7
Configuring application settings

The options available to configure application settings are:

- "Configuring port mirroring," (next)
- "Configuring rate limiting" on page 149
- "Configuring IGMP" on page 151
- "Viewing Multicast group membership configurations" on page 153
- "Creating and managing virtual LANs (VLANs)" on page 155
- "Configuring VLANs" on page 157
- "Configuring broadcast domains" on page 172
- "Viewing VLAN port information" on page 174
- "Managing spanning tree groups" on page 176
- "Configuring ports for spanning tree" on page 181
- "Changing Spanning Tree bridge switch settings" on page 183
- "Configuring MultiLink Trunk (MLT) members" on page 186
- "Monitoring MLT traffic" on page 189

Note: To access the software version 1.2 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Configuring port mirroring

The BPS 2000 supports port mirroring to analyze traffic. You can view existing port mirroring activity and you can configure a specific switch port to mirror up to two specified ports or two MAC addresses. When you configure port mirroring, you have the option to specify either port-based monitoring or address-based monitoring. Refer to *Using the Business Policy Switch 2000 Software Version 1.2* for configuration guidelines for port-mirroring.

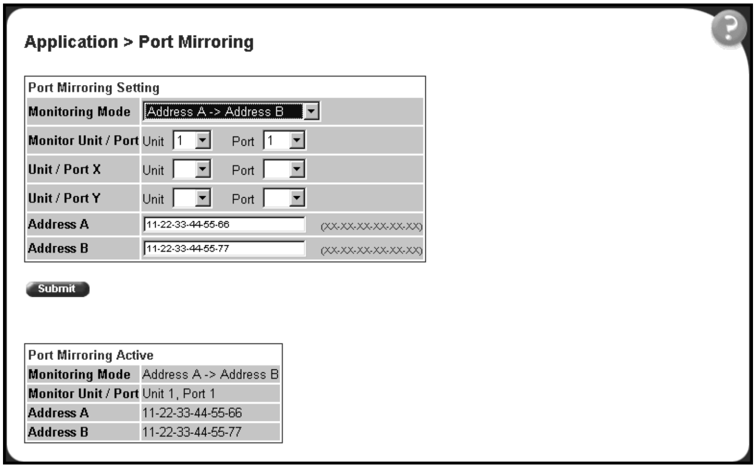
In a stack configuration, you can monitor ports that reside on different units within the stack. For more information, see *Using the Business Policy Switch 2000 Software Version 1.2*.

To configure port mirroring:

1 From the main menu, choose Application > Port Mirroring.

The Port Mirroring page opens (Figure 66).

Figure 66 Port Mirroring page



Application > Port Mirroring

Port Mirroring Setting

Monitoring Mode	Address A -> Address B
Monitor Unit / Port	Unit 1 Port 1
Unit / Port X	Unit Port
Unit / Port Y	Unit Port
Address A	11-22-33-44-55-66 (XX-XX-XX-XX-XX-XX)
Address B	11-22-33-44-55-77 (XX-XX-XX-XX-XX-XX)

Port Mirroring Active

Monitoring Mode	Address A -> Address B
Monitor Unit / Port	Unit 1, Port 1
Address A	11-22-33-44-55-66
Address B	11-22-33-44-55-77

Table 52 describes the items on the Port Mirroring page.

Table 52 Port Mirroring page items

Item	Range	Description
Monitoring Mode	(1) Disabled (2) --> Port X (3) Port X --> (4)<-- --> Port X (5) -->Port X or Port Y --> (6) -->Port X and Port Y --> (7) <-- --> Port X and <-- --> Port Y (8) Address A --> any Address (9) any Address --> Address A (10) <-- --> c Address A (11) Address A --> Address B (12) Address A <-- --> Address B	Choose any one of the six port-based monitoring modes or any one of the five address-based monitoring modes. For more information on selecting one of the six port-based modes that activates the port X and port Y screen fields, where you can choose up to two ports to monitor, see Table 53 on page 148. For more information on selecting one of the five address-based modes that activates the Address A and Address B screen fields, where you can specify MAC addresses to monitor, see Table 54 on page 148. The default setting is Disabled.
Port-based monitoring		
Monitor Port	1..28	Choose the switch port to designate as the monitor port.
Port X	1..28	Choose the first switch port to be monitored by the designated monitor port. This port is monitored according to the value “X” in the Monitoring Mode field.
Port Y	1..28	Choose the second switch port to be monitored by the designated monitor port. This port is monitored according to the value “Y” in the Monitoring Mode field.
Address-based monitoring		
Address A	XX-XX-XX-XX-XX-XX	Type the MAC address to monitor by the designated monitor port. This address is monitored according to the value “Address A” in the Monitoring Mode field.
Address B	XX-XX-XX-XX-XX-XX	Type the MAC address to monitor by the designated monitor port. This address is monitored according to the value “Address B” in the Monitoring Mode field.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Selecting one of the port-based monitoring modes activates the port X and/or the port Y screen fields, where you can choose up to two ports to monitor.

Table 53 describes the port-based monitoring modes.

Table 53 Port-based monitoring modes

Item	Description
Disabled	Choose this option to disable port-based monitoring. The default setting is Disabled.
--> Port X	Choose this option to monitor all traffic received by port X.
Port X -->	Choose this option to monitor all traffic transmitted by port X.
<-- --> Port X	Choose this option to monitor all traffic received and transmitted by port X.
--> Port X or Port Y -->	Choose this option to monitor all traffic received by port X or transmitted by port Y.
--> Port X and Port Y -->	Choose this option to monitor all traffic received by port X (destined to port Y) and then transmitted by port Y (one way conversation steering).
<-- --> Port X and Port Y <-- -->	Choose this option to monitor all traffic received by port X and then transmitted by port Y or transmitted by port X and received by port Y (two way conversation steering).

Selecting any one of the address-based monitoring modes activates the Address A and Address B screen fields, where you can specify MAC addresses to monitor.

Table 54 describes the address-based monitoring modes.

Table 54 Address-based monitoring modes

Item	Description
Disabled	Choose this option to disable port-based monitoring. The default setting is Disabled.
Address A --> any Address	Choose this option to monitor all traffic transmitted from Address A to any address.
any Address --> Address A	Choose this option to monitor all traffic received by Address A from any address.
<-- --> Address A	Choose this option to monitor all traffic received by or transmitted by Address A.
Address A --> Address B	Choose this option to monitor all traffic transmitted by Address A that goes to Address (one way conversation steering).
Address A <-- --> Address B	Choose this option to monitor all traffic received by Address A and then transmitted by Address B or transmitted by Address A and received by Address B (two way conversation steering).

Configuring rate limiting

You can view the current forwarding rate of broadcast and/or multicast packets, and configure the BPS 2000 to limit the forwarding rate of broadcast and multicast packets on each interface. When you configure rate limiting, you are setting the percentage of port bandwidth allowed for a packet type. When the threshold is exceeded, additional packets are discarded.

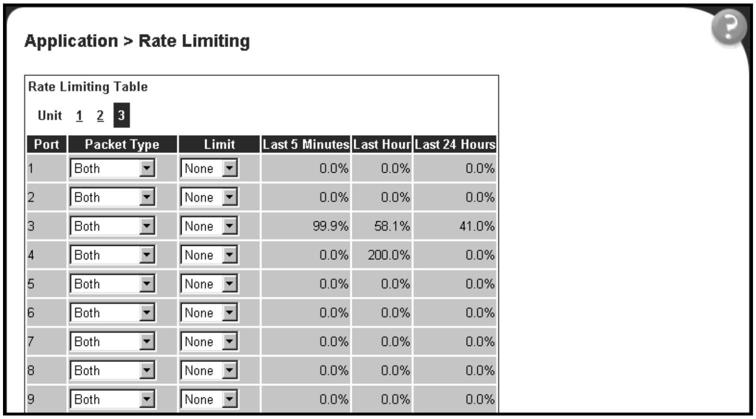
Note: If a port is configured for rate limiting, and it is a MultiLink trunk member, all trunk member ports implement rate limiting. If the port becomes disabled, all trunk members become disabled.

To configure rate limiting:

1 From the main menu, choose Application > Rate Limiting.

The Rate Limiting page opens (Figure 67).

Figure 67 Rate Limiting page



Application > Rate Limiting

Rate Limiting Table

Port	Packet Type	Limit	Last 5 Minutes	Last Hour	Last 24 Hours
1	Both	None	0.0%	0.0%	0.0%
2	Both	None	0.0%	0.0%	0.0%
3	Both	None	99.9%	58.1%	41.0%
4	Both	None	0.0%	200.0%	0.0%
5	Both	None	0.0%	0.0%	0.0%
6	Both	None	0.0%	0.0%	0.0%
7	Both	None	0.0%	0.0%	0.0%
8	Both	None	0.0%	0.0%	0.0%
9	Both	None	0.0%	0.0%	0.0%

Table 55 describes the items on the Rate Limiting page.

Table 55 Rate Limiting page items

Item	Range	Description
Port	1..28	The selected unit's port number. The normal port range is 1 to 28. Note: A standard unit with MDA has a normal range of 25, 26, 28.
Packet Type	(1) Multicast (2) Broadcast (3) Both	Choose the packet type to view on the table. The default setting is Both.
Limit	None, 1-10%	Choose the percentage, if any, of bandwidth allowed for forwarding the packet type specified in the Packet Type field. When the threshold is exceeded, any additional packets are discarded. Note: Rate limiting is disabled if this field is set to none. This allows you to select and view the percentage of specific packet types present in the network, without inadvertently limiting the forwarding rate. The default setting is None.
Last 5 Minutes	0..100%	The percentage of packets received by the port in the last five minutes. This field provides a running average of network activity and is updated every 15 seconds.
Last Hour	0..100%	The percentage of packets received by the port in the last hour. This field provides a running average of network activity and is updated every five minutes.
Last 24 Hours	0..100%	The percentage of packets received by the port in the last 24 hours. This field provides a running average of network activity and is updated every hour.
		Note: The Last 5 Minutes, Last Hour, and Last 24 Hours fields indicate the receiving port's view of network activity regardless of the rate limiting setting.
		Note: When the volume of broadcast and multicast packets is high, placing severe strain on the network (often referred to as a "storm"), you can set the forwarding rate of those packet types to *not exceed* a specified percentage of the total available bandwidth.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

3 Type information in the text boxes, or select from a list.

4 Click Submit.

Note: To avoid broadcast storms (when the volume of a particular packet type is extreme, placing severe strain on the network), set the forwarding rate of the packet type to not exceed a lower percentage of the total available bandwidth.

Configuring IGMP

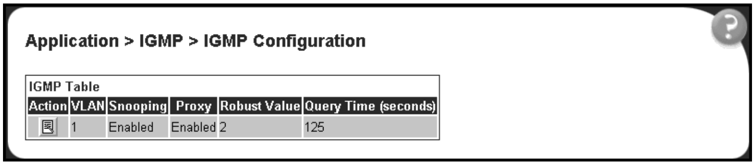
You can configure a VLAN's switch ports to optimize IP multicast packets in a bridged Ethernet environment, and you can view a table of existing IGMP configurations. For more information about IGMP configuration, see *Using the Business Policy Switch 2000* (208700-A).

To configure IGMP:

1. From the main menu, choose Application > IGMP > IGMP Configuration.

   The IGMP Configuration page opens (Figure 68).

Figure 68 IGMP Configuration page



Application > IGMP > IGMP Configuration

IGMP Table

Action	VLAN	Snooping	Proxy	Robust Value	Query Time (seconds)
▤	1	Enabled	Enabled	2	125

Table 56 describes the items on the IGMP Configuration page.

Table 56 IGMP Configuration page items

Item	Description
▤	Displays a modification page for the selected VLAN.
VLAN	The number assigned to the VLAN when the VLAN was created. For more information on creating VLANs, see "Creating and managing virtual LANs (VLANs)" on page 155.
Snooping	The operational status for the IGMP snooping feature.
Proxy	If enabled, this feature allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor. Note: This field affects *all* VLANs.

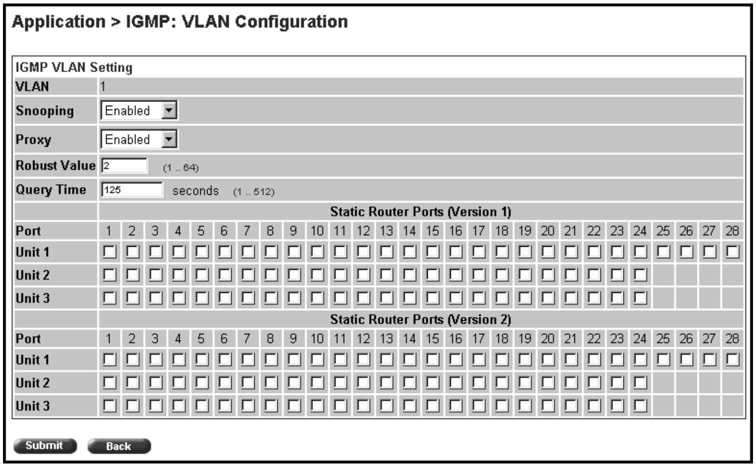
Table 56 IGMP Configuration page items

Item	**Description**
Robust Value	The predetermined value set by the administrator to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value. Note: This field affects *only* the VLAN specified in the page's VLAN field.
Query Time	The query interval (the interval between general queries sent by the multicast router).

2 In the VLAN row of your choice, click the Modify icon.

The IGMP: VLAN Configuration page opens (Figure 69).

Figure 69 IGMP: VLAN Configuration page



Application > IGMP: VLAN Configuration

IGMP VLAN Setting

VLAN 1

Snooping Enabled

Proxy Enabled

Robust Value 2 (1 .. 64)

Query Time 125 seconds (1 .. 512)

	Static Router Ports (Version 1)																											
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				
Unit 3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				

	Static Router Ports (Version 2)																											
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				
Unit 3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				

Table 57 describes the items on the IGMP: VLAN Configuration page.

Table 57 IGMP: VLAN Configuration page items

Item	**Range**	**Description**
VLAN	1..4094	The number assigned to the VLAN when the VLAN was created. For more information on creating VLANs, see "Creating and managing virtual LANs (VLANs)" on page 155.
Snooping	(1) Enabled (2) Disabled	Choose to enable or disable the IGMP snooping feature. Note: This field affects *all* VLANs. The default setting is Enabled.

Table 57 IGMP: VLAN Configuration page items (continued)

Item	**Range**	**Description**
Proxy	(1) Enabled (2) Disabled	Choose to enable or disable the proxy feature. This feature allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor. Note: This field affects *all* VLANs. The default setting is Enabled.
Robust Value	1..64	Type the robust value in the appropriate format. This feature allows you to set the switch to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value. Note: This field affects *only* the VLAN specified in the page's VLAN field. The default settings is 2.
Query Time	1..512	Type the query time (in seconds) in the appropriate format. This feature allows you to control the number of IGMP messages allowed on the subnet by varying the Query Interval (the interval between general queries sent by the multicast router). Note: This field affects *only* the VLAN specified in the page's VLAN field. The default settings is 125 seconds.
Static Router Ports (Version 1 and Version 2)		Click the check boxes of the router ports to associate with the VLAN (alternatively, click the check box to deselect a selected router port). Note: This field affects *all* VLANs.

3. Type information in the text boxes, or select from a list.
4. In the Static Router Ports section(s), click the check boxes of the router ports to associate with the VLAN.
5. Do one of the following:
   - Click Submit.
   - Click Back to return to the IGMP page without making changes.

   The new configuration is displayed in the IGMP Table (Figure 68).

Viewing Multicast group membership configurations

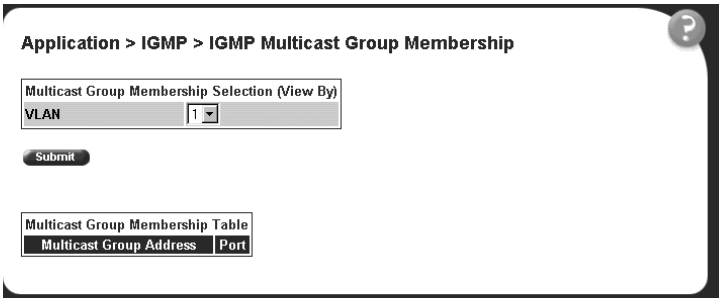
You can view a table configured IP multicast group addresses for a selected VLAN.

To view multicast group membership configurations for a selected VLAN:

1 From the main menu, choose Application > IGMP > IGMP Multicast Group.

The IGMP Multicast Group Membership page opens (Figure 70).

Figure 70 IGMP Multicast Group Membership page



Application > IGMP > IGMP Multicast Group Membership

Multicast Group Membership Selection (View By)

VLAN 1

Multicast Group Membership Table	
Multicast Group Address	Port

Table 58 describes the items on the IGMP Multicast Group Membership page.

Table 58 IGMP Multicast Group Membership page items

Section	Item	Description
Multicast Group Membership Selection (View By)	VLAN	Choose the VLAN on which to view configured IP addresses.
Multicast Group Membership Table	Multicast Group Address	The IP multicast group addresses that are currently active on the associated port.
	Port	The port numbers associated with the IP multicast group addresses displayed in the IP Multicast Group Address field.

2 In the Multicast Group Membership Selection section, choose the number of VLAN on which to view configured IP addresses.

3 Click Submit.

The results are displayed in the Multicast Group Membership Table (Figure 70).

Creating and managing virtual LANs (VLANs)

A VLAN is a collection of switch ports that make up a single broadcast domain. You can configure a VLAN for a single switch, or for multiple switches. When you create a VLAN, you can control traffic flow and ease the administration of moves, adds, and changes on the network, by eliminating the need to change physical cabling.

Note: For guidelines on configuring VLANs, refer to *Using the Business Policy Switch 2000 Software Version 1.2*.

You can configure three types of VLAN in the Web-based management interface:

- Port-based
- Protocol-based
- MAC SA-based

Beginning with software version 1.2, you can use 256 port-, protocol-, and MAC SA-based VLANs for the stack with a Pure BPS 2000 Stack. (The maximum number of MAC SA-based VLANs available is 48). If you are working with a mixed, or Hybrid, stack, you can use 64 VLANs for the entire stack. When you change from a Pure BPS 2000 Stack mode to a Hybrid Stack mode:

- If you have up to 64 VLANs on the Pure BPS 2000 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS 2000 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

Note: To access 256 VLANs, you must be working in Pure BPS 2000 Stack mode. To view and change the stack operational mode, refer to Chapter 3, “Setting system operational modes.”

Port-based VLANs

A port-based VLAN is a VLAN in which the ports are explicitly configured to be in the VLAN. When you create a port-based VLAN on a switch, you assign a VLAN identification number (VLAN ID) and specify which ports belong to the VLAN. The VLAN ID is used to coordinate VLANs across multiple switches.

With software version 1.1 and higher, the automatic PVID feature automatically sets the PVID when you configure a port-based VLAN. The PVID value will be the same value as VLAN. The user can also manually change the PVID value. The default setting for AutoPVID is Off; you must enable this feature.

Protocol-based VLANs

Beginning with software version 1.2, you can configure as many as 255 protocol-based VLANs, with up to 14 different protocols.

A protocol-based VLAN is a VLAN in which the switch ports are configured as members of a broadcast domain, based on the protocol information within a packet. A protocol-based VLAN can localize broadcast traffic and assure that only the protocol-based VLAN ports are flooded with the specified protocol-type packets.

For protocol-based VLANS, the VLAN classification of the frame is dependent on the protocol of the incoming untagged frame. The frame is forwarded only if that VLAN is registered at the egress port.

MAC SA-based VLANs

A MAC source address (SA)-based VLAN is a VLAN whose frame classification is dependent on the MAC SA of the incoming untagged frame. The frame is forwarded only if that VLAN is registered at the egress port.

Configuring VLANs

You can create VLANs by assigning switch ports, MAC SA, and protocols as VLAN members and you can designate an existing VLAN to act as the management VLAN.

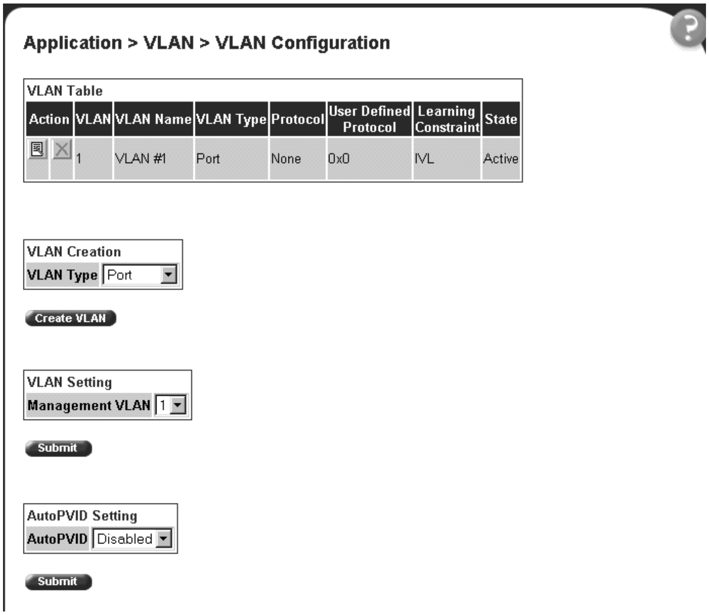
Note: To access the software version 1.2 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

To open the VLAN Configuration page:

➨ From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 71).

Figure 71 VLAN Configuration page



Application > VLAN > VLAN Configuration

VLAN Table

Action	VLAN	VLAN Name	VLAN Type	Protocol	User Defined Protocol	Learning Constraint	State
	1	VLAN #1	Port	None	0x0	IVL	Active

VLAN Creation

VLAN Type Port

VLAN Setting

Management VLAN 1

AutoPVID Setting

AutoPVID Disabled

Table 59 describes the items on the VLAN Configuration page.

Table 59 VLAN Configuration page items

Section	Item	Description
VLAN Table	📝	Displays a modification page.
	✖	Deletes the row.
	VLAN	The number assigned to the VLAN when the VLAN was created.
	VLAN Name	The name assigned to the VLAN when the VLAN was created.
	VLAN Type	The base-type assigned when the VLAN was created. The base types are: Port-based, IP Subnet-based, Protocol-based, and MAC SA-based.
	Protocol	The protocol assigned when the VLAN was created. The protocol types are: IP, IPX 802.2, 1PX 802.3, IPX Snap, IPX Ethernet II, Apple Talk, DEC Lat, SNA 802.2, SNA Ethernet II, Net Bios, XNS, Vines, Ipv6, User Defined, and RARP. For more information, see Table 63 on page 164.
	User Defined Protocol	The user-defined protocol assigned when the VLAN was created.
	Learning Constraint	The type of learning constraint selected when the VLAN was created. The choices are IVL and SVL. Note: If you select IVL, the VLAN uses an independent filtering database from all other VLANs. If you select SVL, the VLAN shares the same filtering database as all other VLANs with SVL. Note: When the stack mode is set to “Pure,” the default setting is IVL; IVL is available *only* with a Pure BPS 2000 stack mode. When the stack mode is set to “Hybrid,” the default setting is SVL.
	State	The current operational state of the VLAN.
VLAN Creation	VLAN Type	Choose the type of VLAN to create and click Create VLAN. Your options are: port-based (page 159), protocol-based (page 162), and MAC SA-based (page 167).
VLAN Setting	Management VLAN	Choose the VLAN to designate as the management VLAN.
AutoPVID Setting	AutoPVID	Choose Enabled to activate the Automatic PVID feature and click Submit. Note: Use this *only* with port-based VLANs.

Creating a port-based VLAN

To create a port-based VLAN:

1 From the main menu choose Application > VLAN > VLAN Configuration.

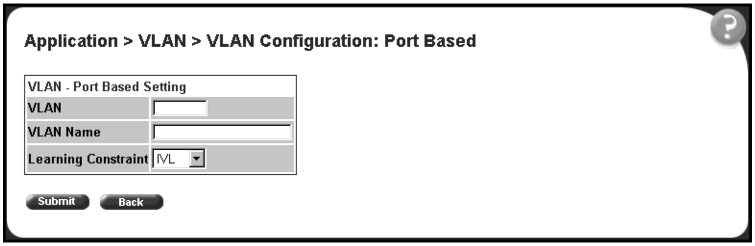
The VLAN Configuration page opens (Figure 71).

2 In the VLAN Creation section, choose Port.

3 Click Create VLAN.

The VLAN Configuration: Port Based setting page opens (Figure 72).

Figure 72 VLAN Configuration: Port Based setting page



Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting

VLAN	
VLAN Name	
Learning Constraint	IVL

Table 60 describes the items on the VLAN Configuration: Port Based setting page.

Table 60 VLAN Configuration: Port Based setting page items

Item	Range	Description
VLAN	1..4094	The number assigned to the VLAN when the VLAN was created.
VLAN Name	1..16	Type a character string to create a unique name to identify the VLAN, for example, VLAN1.
Learning Constraint	(1) IVL (2) SVL	Choose your learning constraint type. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL. Note: If the stack is set to a “pure” operational mode, the default setting is IVL; IVL is available *only* with Pure BPS 2000 stack operational mode. If the stack is set to a “hybrid” operational mode, the default setting is SVL. For more information on setting your stack operational mode, see “Setting system operational modes” on page 112.

4 Type information in the text boxes, or select from a list.

5 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The new port-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page (Figure 71).

Modifying a port-based VLAN

To modify an existing port-based VLAN:

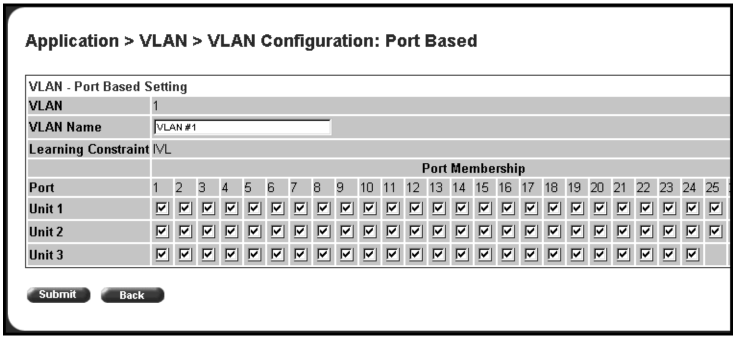
1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 71).

2 In the VLAN Table section, in the port-based VLAN row of your choice, click the Modify icon.

The VLAN Configuration: Port Based modification page opens (Figure 73).

Figure 73 VLAN Configuration: Port Based modification page



Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting

VLAN	1
VLAN Name	VLAN #1
Learning Constraint	IVL

	Port Membership																								
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Unit 1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Unit 2	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Unit 3	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	

Table 61 describes the items on the VLAN Configuration: Port Based modification page.

Table 61 VLAN Configuration: Port Based modification page items

Item	**Description**
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
Learning Constraint	The type of learning constraint selected when the VLAN was created. The learning constraint choices are IVL and SVL. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. IVL is available *only* in the Pure BPS 2000 stack operational mode. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL.
Port/Port Membership	Click the check boxes of *standalone or stacked unit* ports to associate it with the VLAN or, if the port is already a member, click the check box to deselect the it as a member of the VLAN. A port can be configured in one or more VLANs. This field is dependent on the Tagging field value in the VLAN Port Configuration screen. For example: • When the Tagging field is set to *Untagged Access*, you can set the Port Membership field as an untagged port member or as a non-VLAN port member. • When the Tagging field is set to *Tagged Trunk*, you can set the Port Membership field as a tagged port member or as a non-VLAN port member.

3 Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.

4 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table (Figure 71).

Creating a protocol-based VLAN

To create a protocol-based VLAN:

1 From the main menu, choose Application > VLAN > VLAN Configuration.

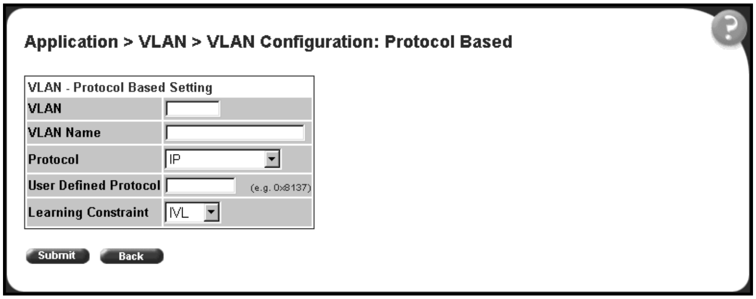
The VLAN Configuration page opens (Figure 71).

2 In the VLAN Creation section, choose Protocol.

3 Click Create VLAN.

The VLAN Configuration: Protocol Based setting page opens (Figure 74).

Figure 74 VLAN Configuration: Protocol Based setting page



Application > VLAN > VLAN Configuration: Protocol Based

VLAN - Protocol Based Setting		
VLAN		
VLAN Name		
Protocol	IP	
User Defined Protocol		(e.g. 0x8137)
Learning Constraint	IVL	

Table 62 describes the items on the VLAN Configuration: Protocol Based setting page.

Note: Beginning with software version 1.2, there are 14 available protocols.

Table 62 VLAN Configuration: Protocol Based setting page items

Item	**Range**	**Description**
VLAN	1..4094	Type a unique number to identify the VLAN.
VLAN Name	1..16	Type a unique name to identify the VLAN.
Protocol	IP, IPX 802.2, 1PX 802.3, IPX Snap, IPX Ethernet II, Apple Talk, DEC Lat, SNA 802.2, SNA Ethernet II, Net Bios, XNS, Vines, Ipv6, User Defined, and RARP.	Choose the supported protocol for the VLAN. For more information, see Table 63 on page 164.
User Defined Protocol		If you selected “User Defined” from the Protocol pulldown list, specify the protocol identifier for the VLAN. Note: Any frames that match the specified PID, in any of the following ways are assigned to that user defined VLAN: • The ethertype for Ethernet type 2 frames • The PID in Ethernet SNAP frames • The DSAP or SSAP value in Ethernet 802.2 frames. For a list of rereserved PIDs that are unavailable for user-defined PIDs, see Table 64 on page 165.
Learning Constraint	(1) IVL (2) SVL	Choose your learning constraint type. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL. Note: If the stack is set to a “pure” operational mode, the default setting is IVL; IVL is available *only* in Pure BPS 2000 stack operational mode. If the stack is set to a “hybrid” operational mode, the default setting is SVL. For more information on setting your stack operational mode, see “Setting system operational modes” on page 112.

4 Type information in the text boxes, or select from a list.

5 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The new protocol-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page (Figure 71).

Caution: Gigabit ports and BayStack 410 ports do not have the ability to assign incoming untagged frames to a protocol-based VLAN. To allow gigabit ports and BayStack 410 ports to participate in protocol-based VLANs, set the tagging field value to “Tagged Trunk” (see “Configuring broadcast domains” on page 172).

Table 63 defines the standard protocol-based VLANs and PID types that are supported by the Business Policy Switch and BayStack 450 and 410 switches. See Table 64 for a list of rereserved PIDS that are not available for user-defined PIDs.

Table 63 Standard protocol-based VLANs and PID types

PID Name	**Encapsulation**	**PID Value (hex)**	**VLAN Type**
IP Ether2	Ethernet type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
Ipx 802.3	Ethernet 802.2	FF FF	Novell IPX on Ethernet 802.3 frames
Ipx 802.2	Ethernet 802.0	E0 E0	Novell IPX on Ethernet 802.2 frames
Ipx Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames
Ipx Ethernet II	Ethernet type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
Apple Talk	Ethernet type 2 or Ethernet Snap	809B, 80F3	AppleTalk on Ethernet Type 2 and Ethernet Snap frames
DEC Lat	Ethernet type 2	6004	DEC LAT protocol
DEC Other	Ethernet type 2	6000 - 6003, 6005 - 6009, 8038	Other DEC protocols
Sna 802.2	Ethernet 802.2	04**, **04	IBM SNA on IEEE 802.2 frames
Sna Ethernet II	Ethernet type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios	Ethernet type 2	F0**, **F0	NetBIOS protocol
XNS	Ethernet type 2	0600, 0807	Xerox XNS
Vines	Ethernet type 2	0BAD	Banyan VINES
IPv6	Ethernet type 2	86DD	IP version 6

Table 63 Standard protocol-based VLANs and PID types (continued)

PID Name	Encapsulation	PID Value (hex)	VLAN Type
RARP	Ethernet type 2	8035	Reverse Address Resolution Protocol (RARP): RARP is a protocol used by some old diskless devices to obtain IP addresses by providing the MAC layer address. When you create a VLAN based on RARP, you can limit the RARP broadcasts to the ports that lead to the RARP server.
User-Defined	Ethernet type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16 bit value	If you select "User Defined" from the Protocol pulldown list, specify the protocol identifier for the VLAN. Note: Any frames that match the specified PID, in any of the following ways are assigned to that user defined VLAN: The ethertype for Ethernet type 2 frames The PID in Ethernet SNAP frames The DSAP or SSAP value in Ethernet 802.2 frames. For a list of rereserved PIDs that are unavailable for user-defined PIDs, see Table 63 on page 164

Table 64, describes the PIDS that are reserved and not available for user-defined PIDs.

Table 64 Predefined Protocol Identifier (PID)

PID Name	Encapsulation	PID Value (hex)	VLAN Type
IP Ether2	Ethernet type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
Ipx 802.3	Ethernet 802.2	FF FF	Novell IPX on Ethernet 802.3 frames
Ipx 802.2	Ethernet 802.0	E0 E0	Novell IPX on Ethernet 802.2 frames
Ipx Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames
Ipx Snap2	Ethernet type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
AplTk Ether2 Snap	Ethernet type 2 or Ethernet Snap	809B, 80F3	AppleTalk on Ethernet Type 2 and Ethernet Snap frames
Declat Ether2	Ethernet type 2	6004	DEC LAT protocol
DecOther Ether2	Ethernet type 2	6000 - 6003, 6005 - 6009, 8038	Other DEC protocols
Sna 802.2	Ethernet 802.2	04**, **04	IBM SNA on IEEE 802.2 frames
Sna Ether2	Ethernet type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios 802.2	Ethernet type 2	F0**, **F0	NetBIOS protocol
Xns Ether2	Ethernet type 2	0600, 0807	Xerox XNS

Table 64 Predefined Protocol Identifier (PID) (continued)

Vines Ether2	Ethernet type 2	0BAD	Banyan VINES
Ipv6 Ether2	Ethernet type 2	86DD	IP version 6
User-Defined	Ethernet type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16 bit value	User-defined protocol-based VLAN. For a list of rereserved PIDs that are unavailable for user-defined PIDs, see Table 64 on page 165.

Modifying a protocol-based VLAN

To modify an existing port-based VLAN:

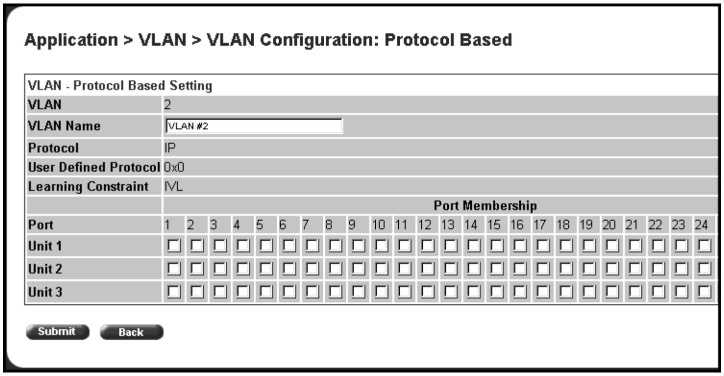
1. From the main menu, choose Application > VLAN > VLAN Configuration.

   The VLAN Configuration page opens (Figure 71).

2. In the VLAN Table section, in the protocol-based VLAN row of your choice, click the Modify icon.

   The VLAN Configuration: Protocol Based modification page opens (Figure 75).

Figure 75 VLAN Configuration: Protocol Based modification page



Application > VLAN > VLAN Configuration: Protocol Based

VLAN - Protocol Based Setting

VLAN	2
VLAN Name	VLAN #2
Protocol	IP
User Defined Protocol	0x0
Learning Constraint	IVL

	Port Membership																							
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Table 65 describes the items on the VLAN Configuration: Protocol Based modification page.

Table 65 VLAN Configuration: Protocol Based modification page items

Item	Description
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
Learning Constraint	The type of learning constraint selected when the VLAN was created. The learning constraint choices are IVL and SVL. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. IVL is available *only* in Pure BPS 2000 stack operational mode.If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL.
Port/Port Membership	Click the check boxes beneath a port to associate the port with the VLAN or, if the port is already selected click the check box to deselect the port as a member of the VLAN.

3 Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.

4 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table (Figure 71).

Creating a MAC SA-based VLAN

To create a MAC SA-based VLAN:

1 From the main menu, choose Application > VLAN > VLAN Configuration.

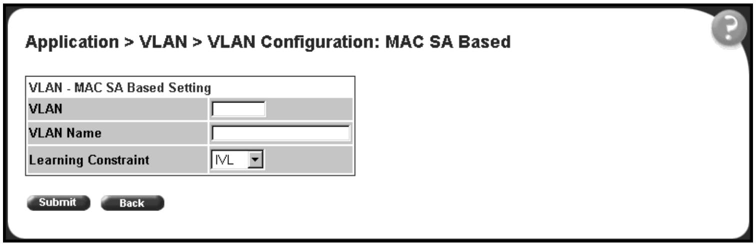
The VLAN Configuration page opens (Figure 71).

2 In the VLAN Creation section, choose MAC SA.

3 Click Create VLAN.

The VLAN Configuration: MAC SA Based setting page opens (Figure 76).

Figure 76 VLAN Configuration: MAC SA Based setting page


Application > VLAN > VLAN Configuration: MAC SA Based
VLAN - MAC SA Based Setting
VLAN
VLAN Name
Submit
Back

Learning Constraint: IVL

Table 66 describes the items on the VLAN Configuration: MAC SA Based setting page.

Table 66 VLAN Configuration: MAC SA Based setting page items

Item	Range	Description
VLAN	1..4094	Type a unique number to identify the VLAN.
VLAN Name	1..16	Type a unique name to identify the VLAN, for example *.
Learning Constraint	(1) IVL (2) SVL (default)	Choose your learning constraint type. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL. Note: If the stack is set to a “pure” operational mode, the default setting is IVL; IVL is available *only* in Pure BPS 2000 mode. If the stack is set to a “hybrid” operational mode, the default setting is SVL. For more information on setting your stack operational mode, see “Setting system operational modes” on page 112.

4 Type information in the text boxes, or select from a list.

5 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The new MAC SA-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page (Figure 71).

Modifying a MAC SA-based VLAN

To modify an existing MAC SA-based VLAN:

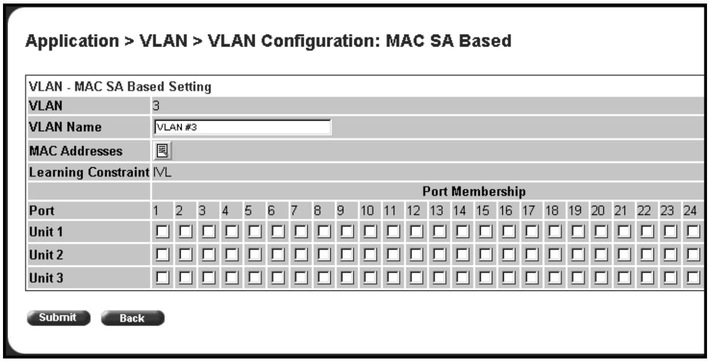
1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 71).

2 In the VLAN Table section, in the MAC SA-based VLAN row of your choice, click the Modify icon.

The VLAN Configuration: MAC SA Based modification page opens (Figure 77).

Figure 77 VLAN Configuration: MAC SA Based modification page



Application > VLAN > VLAN Configuration: MAC SA Based

VLAN - MAC SA Based Setting	
VLAN	3
VLAN Name	VLAN #3
MAC Addresses	
Learning Constraint	IVL

	Port Membership																							
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Table 67 describes the items on the VLAN Configuration: MAC SA Based modification page.

Table 67 VLAN Configuration: MAC SA Based modification page items

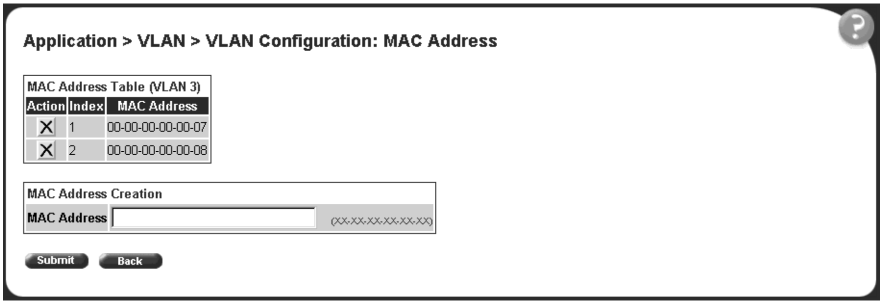
Item	**Description**
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
📝	Opens the VLAN Configuration: MAC Address page (Figure 78).
Learning Constraint	The type of learning constraint selected when the VLAN was created. The learning constraint choices are IVL and SVL. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. IVL is available *only* in the Pure BPS 2000 stack operational mode. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL.

3 Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.

4 To create MAC address associations, click the modify icon.

The VLAN Configuration: MAC Address page opens (Figure 78).

Figure 78 VLAN Configuration: MAC Address page



Application > VLAN > VLAN Configuration: MAC Address

MAC Address Table (VLAN 3)

Action	Index	MAC Address
☒	1	00-00-00-00-00-07
☒	2	00-00-00-00-00-08

MAC Address Creation

MAC Address ▭ (XX-XX-XX-XX-XX-XX)

5 In the MAC Address Creation section, type the MAC address to associate with the VLAN.

The MAC address appears in the MAC Address Table (Figure 78).

Note: You can delete an existing MAC address by clicking the delete icon in the row of the MAC address you want to delete.

---

6 Do one of the following:

- Click Submit to save your changes and return to the VLAN Configuration: MAC SA Based setting page.
- Click Back to return to the VLAN Configuration: MAC SA Based setting page without making changes.

7 On the VLAN Configuration: MAC SA Based setting page, do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table (Figure 71).

Selecting a management VLAN

You can select any VLAN to perform as the management VLAN. VLAN 1 is the default management VLAN for the switch. To set this field, the VLAN State field value must be active.

To select a VLAN as the management VLAN:

1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 71).

2 In the VLAN Setting section, choose the VLAN to assign as your management VLAN.

3 Click Submit.

Deleting a VLAN configuration

To delete a VLAN configuration:

1. From the main menu, choose Application > VLAN > VLAN Configuration.

   The VLAN Configuration page opens (Figure 71).

2. In the VLAN Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:

   - Click Yes to delete the VLAN configuration.
   - Click Cancel to return to the VLAN Configuration page without making changes.

Note: You cannot delete VLAN 1.

Configuring broadcast domains

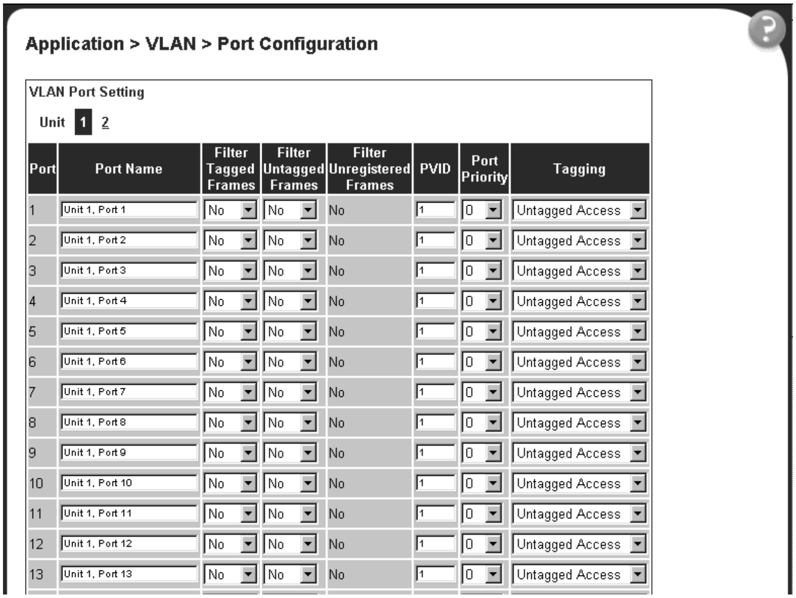
You can configure specified VLAN switch ports with the appropriate PVID/VLAN association that enables the creation of broadcast domains. If you have enabled automatic PVID, you can change the PVID number on this screen. You can configure specified switch ports to filter (discard) all received tagged frames, untagged frames, or unregistered frames. You can also prioritize the order in which the switch forwards untagged packets, on a per-port basis.

To configure broadcast domains:

1. From the main menu, choose Application > VLAN > Port Configuration.

   The Port Configuration page opens (Figure 79).

Figure 79 Port Configuration page



Application > VLAN > Port Configuration

VLAN Port Setting

Unit **1** 2

Port	Port Name	Filter Tagged Frames	Filter Untagged Frames	Filter Unregistered Frames	PVID	Port Priority	Tagging
1	Unit 1, Port 1	No	No	No	1	0	Untagged Access
2	Unit 1, Port 2	No	No	No	1	0	Untagged Access
3	Unit 1, Port 3	No	No	No	1	0	Untagged Access
4	Unit 1, Port 4	No	No	No	1	0	Untagged Access
5	Unit 1, Port 5	No	No	No	1	0	Untagged Access
6	Unit 1, Port 6	No	No	No	1	0	Untagged Access
7	Unit 1, Port 7	No	No	No	1	0	Untagged Access
8	Unit 1, Port 8	No	No	No	1	0	Untagged Access
9	Unit 1, Port 9	No	No	No	1	0	Untagged Access
10	Unit 1, Port 10	No	No	No	1	0	Untagged Access
11	Unit 1, Port 11	No	No	No	1	0	Untagged Access
12	Unit 1, Port 12	No	No	No	1	0	Untagged Access
13	Unit 1, Port 13	No	No	No	1	0	Untagged Access

Table 68 describes the items on the Port Configuration page.

Table 68 Port Configuration page items

Item	Range	Description
Port	1..28	The port number.
Port Name	1..16	Type character string to create a unique port name, for example, Unit 1, Port 1.
Filter Tagged Frames	(1) Yes (2) No	Choose how to process filter tagged frames. When a flag is set (Yes), the frames are discarded by the forwarding process. When the flag is reset, the frames are processed normally. The default setting is No (frames are not discarded).
Filter Untagged Frames	(1) Yes (2) No	Choose how to process filter untagged frames. When a flag is set, the frames are discarded by the forwarding process. The default setting is No (no frames discarded).
Filter Unregistered Frames	(1) Yes (2) No	Displays yes/no if a flag is set. If yes, unregistered frames are discarded by the forwarding process. When the flag is reset, unregistered frames are processed normally. The default settings is No.

Table 68 Port Configuration page items (continued)

Item	Range	Description
PVID	1..4094	Type the number of the VLAN ID to assign to untagged frames received on this trunk port. For example, a port with a PVID of 3 assigns all untagged frames received on this port to VLAN 3. The default setting is 1. Note: If AutoPVID is enabled and you want another PVID, enter the desired PVID here.
Port Priority	0-7	Choose the level of priority for each port.
Tagging	(1) Untagged Access (2) Tagged Trunk	Choose the tagging for each port.

2. In the upper-left hand corner, click on the unit number of the switch to monitor.
3. Type information in the text boxes, or select from a list.
4. Click Submit.

Viewing VLAN port information

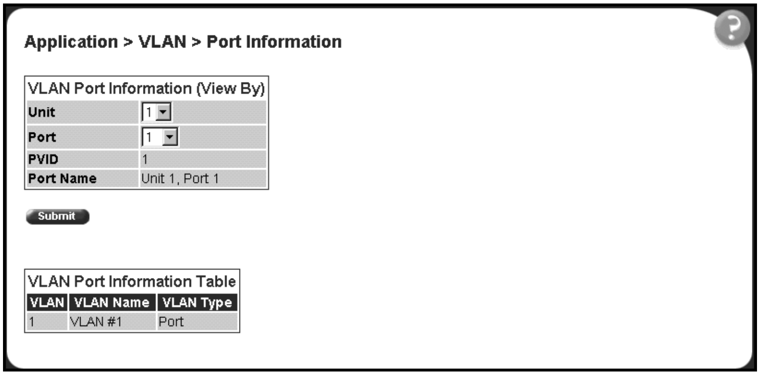
You can view VLAN information about a selected switch port.

To view VLAN port information:

1. From the main menu, choose Application > VLAN > Port Information.

   The Port Information page opens (Figure 80).

Figure 80 Port Information page



Application > VLAN > Port Information

VLAN Port Information (View By)	
Unit	1
Port	1
PVID	1
Port Name	Unit 1, Port 1

VLAN Port Information Table

VLAN	VLAN Name	VLAN Type
1	VLAN #1	Port

Table 69 describes the items on the Port Information page.

Table 69 Port Information page items

Section	Item	Range	Description
VLAN Port Information (View By)	Unit	1..8	Choose the number of the switch to view.
	Port	1..28	Choose the number of the switch's port to view.
	PVID		The PVID assigned when the VLAN port was created.
	Port Name		The port name assigned when the VLAN port was created.
VLAN Port Information Table	VLAN		The number assigned to the VLAN when it was created.
	VLAN Name		The name assigned to the VLAN when it was created.
	VLAN Type		The VLAN type assigned to the VLAN when it was created.

2. In the VLAN Port Information (View By) section, enter the unit and port number of the VLAN you want to view.
3. Click Submit.

   The results of your request are displayed in the VLAN Port Information Table (Figure 80).

Managing spanning tree groups

You can configure system parameters for Spanning Tree Protocol, the industry standard for avoiding loops in switched networks. You can configure individual switch ports or all switch ports for participation in the spanning tree algorithm (STA).

➡ **Note:** STP resolves duplicate paths in networks and is not necessary for ports that have workstations directly attached to the switch. When STP is enabled on these ports (the default), workstations are unable to attach to servers for a few seconds while STP stabilizes.

With software version 1.2 and higher, the BPS 2000 supports multiple instances (8) of spanning tree groups (STGs) running simultaneously, either all in one standalone switch or across a Pure BPS 2000 Stack. Each STG sends its own Bridge Protocol Data Units (BPDUs), and each STG must be independently configured.

➡ **Note:** You must be in Pure BPS 2000 Stack mode in the Stack Operational Mode screen to enable more than 1 STG. If you change to Hybrid mode, you lose all but the default STG.

In the default configuration of the BPS 2000, a single STG with the ID of 1 includes all ports on the switch. It is called the Default STG and sends only untagged BPDUs in order to operate with all devices that support only one instance of STP. Although ports can be added to or deleted from the Default STG, the Default STG itself **cannot** be deleted from the system. All other STGs, except the Default STG, must be created by the user.

➡ **Note:** To become active, each STG must be enabled by the user after creation. For guidelines on configuring, refer to *Using the Business Policy Switch 2000 Software Version 1.2*.

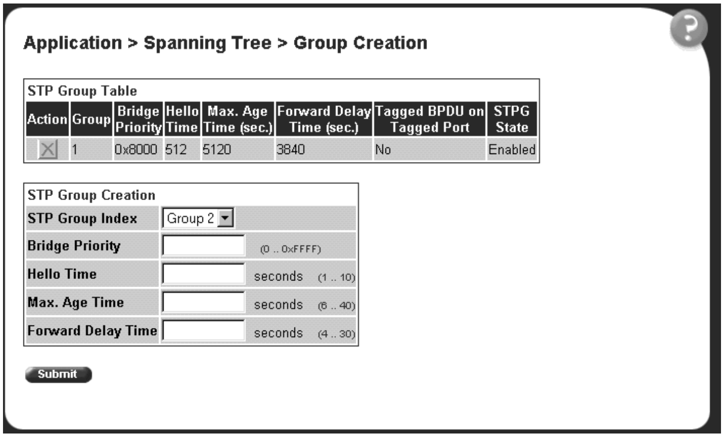
Creating spanning tree groups

To configure spanning tree groups:

1 From the main menu, choose Application > Spanning Tree > Group Creation.

The Group Creation page opens (Figure 81).

Figure 81 Spanning Tree Group Creation page



Application > Spanning Tree > Group Creation

STP Group Table

Action	Group	Bridge Priority	Hello Time	Max. Age Time (sec.)	Forward Delay Time (sec.)	Tagged BPDU on Tagged Port	STPG State
☒	1	0x8000	512	5120	3840	No	Enabled

STP Group Creation

STP Group Index	Group 2 ▾	
Bridge Priority		(0 .. 0xFFFF)
Hello Time		seconds (1 .. 10)
Max. Age Time		seconds (6 .. 40)
Forward Delay Time		seconds (4 .. 30)

Table 70 describes the items on the Spanning Tree Group Creation page.

Table 70 Spanning Tree Group Creation page items

Section	Item	Description
STP Group Table	☒	Deletes the group.
	Group	The number assigned to the spanning tree group when the group was created.
	Bridge Priority	For the STP Group, indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The spanning tree algorithm uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values.

Table 70 Spanning Tree Group Creation page items

Section	Item	Description
	Hello Time	For the STP Group, indicates the Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note that, although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network.
	Max. Age time (sec.)	For the STP Group, specifies the maximum age (in seconds) that a Hello message can attain before it is discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. Note that, if this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.
	Forward Delay Time (sec.)	For the STP Group indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note that all bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value.
	Tagged BPDU on Tagged Port	Allows you to choose to send either tagged or untagged BPDUs from a tagged port.
	STPG State	The current operational state of the spanning tree group: Enabled or Disabled.
STP Group Creation	STP Group Index	Choose the group number you want to create.
	Bridge Priority	Enter the priority you want.
	Hello Time	Enter the hello time you want for this STG in seconds; range is 1 to 10.
	Max. Age time (sec.)l	Enter the maximum age time you want for this STG in seconds; range is 6 to 40.
	Forward Delay Time (sec.)	Enter the forward delay time you want for this STG in seconds; range is 4 to 30.

2 Complete the fields as shown.

3 Click Submit.

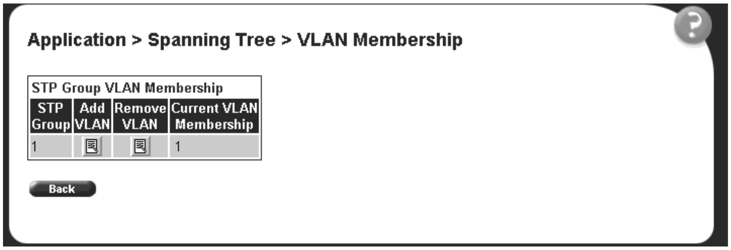
Associating STG with VLAN membership

To add a VLAN to an STG:

1 From the main menu, choose, Application > Spanning Tree > VLAN Membership.

The Spanning Tree VLAN Membership page opens (Figure 82).

Figure 82 Spanning Tree VLAN Membership page



Application > Spanning Tree > VLAN Membership

STP Group VLAN Membership

STP Group	Add VLAN	Remove VLAN	Current VLAN Membership
1	🗎	🗎	1

The table displays the spanning tree group and the current VLAN membership.

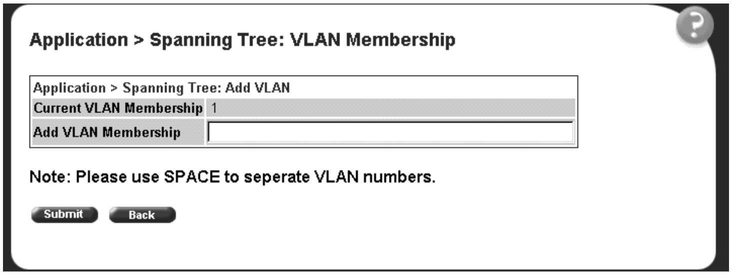
You can add or remove one or more VLANs to an STG.

2 To add a VLAN:

- a Click the modification icon in the Add VLAN column.

  The Spanning Tree VLAN Membership Add VLAN page opens (Figure 83).

Figure 83 Spanning Tree Add VLAN page



Application > Spanning Tree: VLAN Membership

Application > Spanning Tree: Add VLAN	
Current VLAN Membership	1
Add VLAN Membership	

Note: Please use SPACE to seperate VLAN numbers.

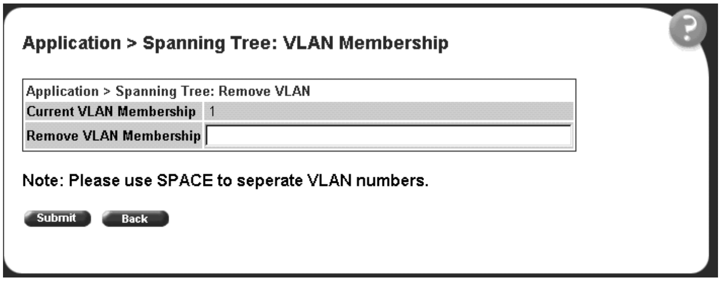
- b Enter the number of the VLAN(s) you want to add to the STG.
- c Click Submit.

3 To remove a VLAN:

  a Click the modification icon in the Remove VLAN column.

  The Spanning Tree VLAN Membership Remove VLAN page opens (Figure 84).

Figure 84 Spanning Tree Remove VLAN page



Application > Spanning Tree: VLAN Membership

Application > Spanning Tree: Remove VLAN	
Current VLAN Membership	1
Remove VLAN Membership	

Note: Please use SPACE to seperate VLAN numbers.

  b Enter the number of the VLAN(s) you want to remove to the STG.

  c Click Submit.

Note: You cannot delete VLAN 1 from STG 1.

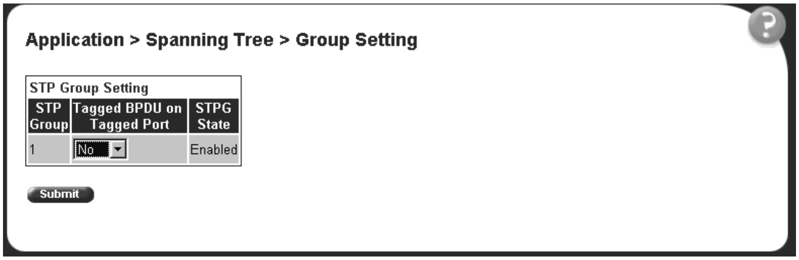
Configuring the STG

To configure an STG:

1 From the main menu, choose Applications > Spanning Tree > Group Setting.

The Spanning Tree Group Setting page opens (Figure 85).

Figure 85 Spanning Tree Group Setting page



Application > Spanning Tree > Group Setting

STP Group Setting

STP Group	Tagged BPDU on Tagged Port	STPG State
1	No	Enabled

2 The STP Group number is displayed.

3 Use the Tagged BPDU on Tagged port field to set the frames as tagged (Yes) or untagged on tagged ports (No).

4 The STPG State displays status of the STP group.

5 Click Submit.

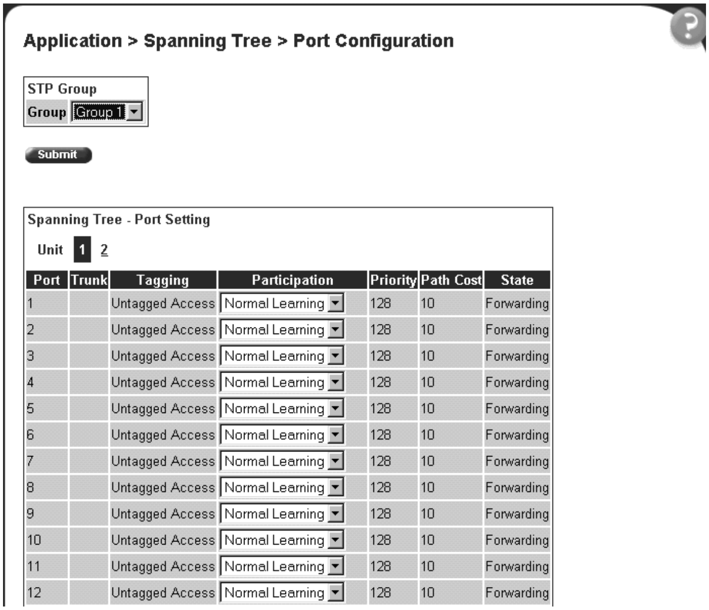
Configuring ports for spanning tree

To configure switch ports for Spanning Tree participation:

1 From the main menu, choose Application > Spanning Tree > Port Configuration.

The Spanning Tree Port Configuration page opens (Figure 86).

Figure 86 Spanning Tree Port Configuration page



Application > Spanning Tree > Port Configuration

STP Group

Group: Group 1

Spanning Tree - Port Setting

Unit 1 2

Port	Trunk	Tagging	Participation	Priority	Path Cost	State
1		Untagged Access	Normal Learning	128	10	Forwarding
2		Untagged Access	Normal Learning	128	10	Forwarding
3		Untagged Access	Normal Learning	128	10	Forwarding
4		Untagged Access	Normal Learning	128	10	Forwarding
5		Untagged Access	Normal Learning	128	10	Forwarding
6		Untagged Access	Normal Learning	128	10	Forwarding
7		Untagged Access	Normal Learning	128	10	Forwarding
8		Untagged Access	Normal Learning	128	10	Forwarding
9		Untagged Access	Normal Learning	128	10	Forwarding
10		Untagged Access	Normal Learning	128	10	Forwarding
11		Untagged Access	Normal Learning	128	10	Forwarding
12		Untagged Access	Normal Learning	128	10	Forwarding

Table 71 describes the items on the Spanning Tree Port Configuration page.

Table 71 Spanning Tree Port Configuration page items

Section	Item	Description
STP Group	Group	Choose the STG Group you want to view.
Spanning Tree - Port Setting	Port	The port number of the currently displayed unit.
	Trunk	The trunk that corresponds to the switch ports specified as MLT members.
	Tagging	Displays whether the port is a tagged or an untagged port.
	Participation	Choose any (or all) of the switch ports for Spanning Tree participation.Your options are: (1) Normal Learning (2) Fast Learning (3) Disabled Note: When an individual port is a trunk member, changing this setting for one of the trunk members changes the setting for all members of that trunk. Consider the effect changing this value has in your network topology before making changes. The default settings is Normal Learning.
	Priority	The bridge spanning tree parameter that prioritizes the port's lowest path cost to the root. When one or more ports have the same path cost, the STA selects the path with the highest priority (lowest numerical value).

Table 71 Spanning Tree Port Configuration page items

Section	Item	Description
	Path Cost	The bridge spanning tree parameter that determines the lowest path cost to the root.
	State	The current state of the port as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. Note: If the bridge has detected a port that is malfunctioning, it will place that port into the broken (6) state. For ports which are disabled, this object will have a value of disabled (1).

2. Using the Spanning Tree - Port Settings fields, in the port row(s) of your choice, choose to enable STP (normal learning or fast learning) or disable STP.
3. Click Submit.

Changing Spanning Tree bridge switch settings

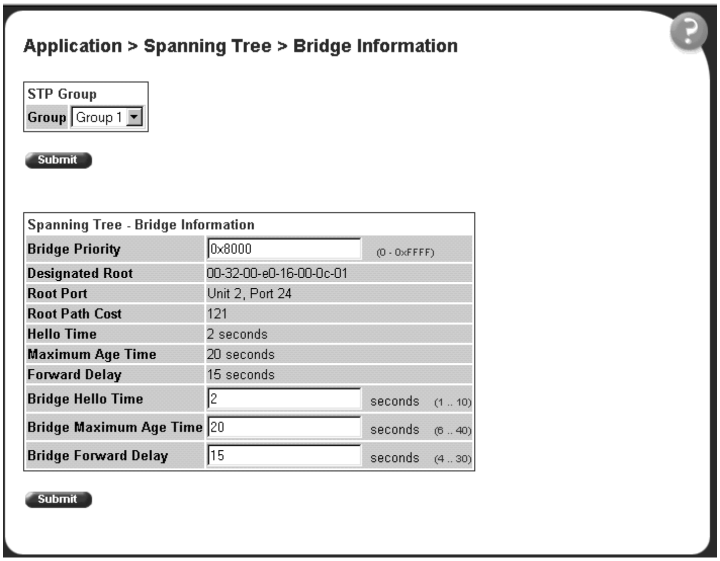
You can view and configure existing Spanning Tree switch settings.

To configure Spanning Tree switch settings:

1. From the main menu, choose Application > Spanning Tree > Bridge Information.

   The Spanning Tree Bridge Information page opens (Figure 87).

Figure 87 Spanning Tree Bridge Information page



Application > Spanning Tree > Bridge Information

STP Group	
Group	Group 1

Spanning Tree - Bridge Information		
Bridge Priority	0x8000	(0 - 0xFFFF)
Designated Root	00-32-00-e0-16-00-0c-01	
Root Port	Unit 2, Port 24	
Root Path Cost	121	
Hello Time	2 seconds	
Maximum Age Time	20 seconds	
Forward Delay	15 seconds	
Bridge Hello Time	2	seconds (1 .. 10)
Bridge Maximum Age Time	20	seconds (6 .. 40)
Bridge Forward Delay	15	seconds (4 .. 30)

Table 72 describes the items on the Spanning Tree Bridge Information page.

Table 72 Spanning Tree Bridge Information page items

Section	**Item**	**Range**	**Description**
STP Group	Group		Choose the STP Group you want to work with.
Spanning Tree - Bridge Information	Bridge Priority	0..65535	Type the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The Spanning Tree Algorithm uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses. The default setting is 8000.
	Designated Root	XXXXXXX XXXXXXX	The bridge ID of the root bridge, as determined by the Spanning Tree Algorithm.
	Root Port	1..28	The port number of the port which offers the lowest cost past from this bridge to the root bridge.
	Root Path Cost	Integer	The cost of the path to the root as seen from this bridge.
	Hello Time	1..10 seconds	The actual Hello Interval, the amount of time between transmissions of configuration Bridge Protocol Data Units (BPDUs) that the root bridge is currently using. Note: Bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. See also Bridge Hello Time.

Table 72 Spanning Tree Bridge Information page items

Section	Item	Range	Description
	Maximum Age Time	6..40 seconds	The Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before it is discarded. Note: The root bridge's Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. See also Bridge Maximum Age Time.
	Forward Delay	4..30 seconds	The Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note: The root bridge's Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network. See also Bridge Forward Delay.
	Bridge Hello Time	1..10 seconds	The Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note: Although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. See also Hello Time. The default setting is 2 seconds.
	Bridge Maximum Age Time	6..40 seconds	The maximum age (in seconds) that a Hello message can attain before it is discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. Note: If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. See also Maximum Age Time. The default setting is 20 seconds.
	Bridge Forward Delay	4..30 seconds	The amount of time that the bridge ports remains in the Listening and Learning states before entering the Forwarding state. Note: All bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value. See also Forward Delay. The default setting is 15 seconds.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Configuring MultiLink Trunk (MLT) members

You can configure groups of links between the BPS 2000 and another switch or a server to provide higher bandwidth with active redundant links. Trunked ports can span multiple units of the stack for fail-safe connectivity to mission-critical servers and the network center.

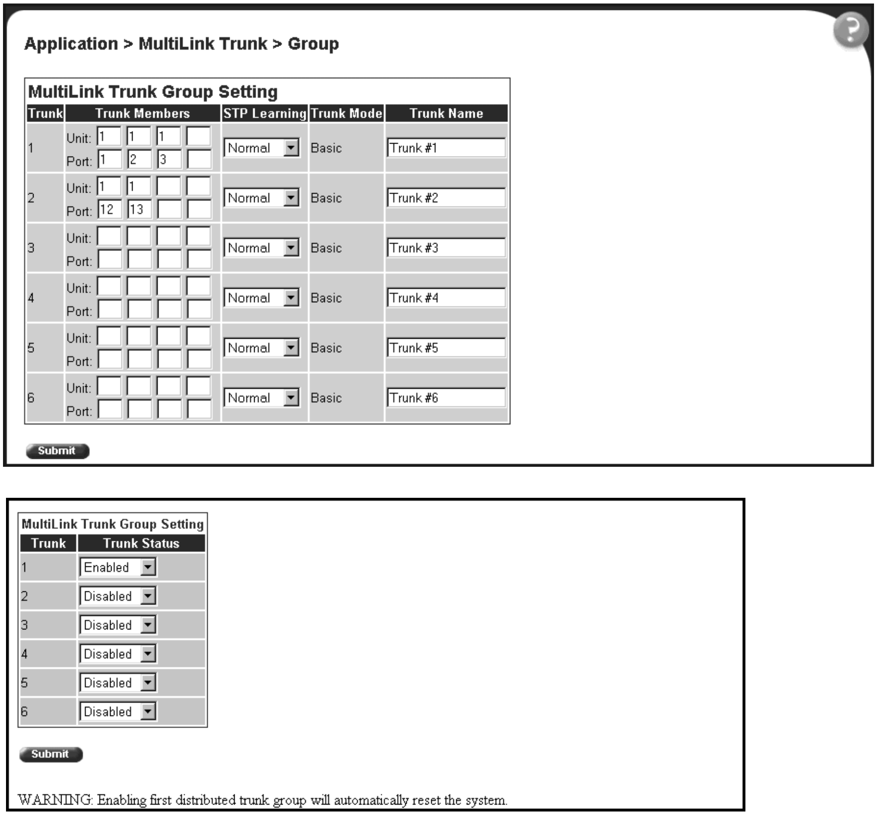
You can configure two to four switch ports together as members of a trunk to a maximum of six trunks.

To configure MultiLink Trunk members:

1 From the main menu, choose Application > MultiLink Trunk > Group.

The Group page opens (Figure 88).

Figure 88 Group page



Application > MultiLink Trunk > Group

MultiLink Trunk Group Setting

Trunk	Trunk Members	STP Learning	Trunk Mode	Trunk Name
1	Unit: 1 1 1 Port: 1 2 3	Normal	Basic	Trunk #1
2	Unit: 1 1 Port: 12 13	Normal	Basic	Trunk #2
3	Unit: Port:	Normal	Basic	Trunk #3
4	Unit: Port:	Normal	Basic	Trunk #4
5	Unit: Port:	Normal	Basic	Trunk #5
6	Unit: Port:	Normal	Basic	Trunk #6

MultiLink Trunk Group Setting

Trunk	Trunk Status
1	Enabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled

WARNING: Enabling first distributed trunk group will automatically reset the system.

Table 73 describes the items on the Group page.

Table 73 Group page items

Section	Item	Range	Description
MultiLink Trunk Group Setting	Trunk	1..6	This column contains fields in each row that can be configured to create the corresponding trunk. The Unit value in the (Unit/Port) field is configurable only when the switch (unit) is part of a stack configuration. It indicates that the trunk members in this row are associated with the specified unit number configured in the Unit field. Each switch port can only be a member of a single trunk. The appropriate trunk number for each trunk member configured within this field is shown adjacent to the corresponding switch port on the following management pages: Port Configuration (see Figure 40 on page 102) and Spanning Tree Configuration (see Figure 79 on page 173). There are no default settings.
	Trunk Port Members	Unit: 1..8 Port: 1..28	Type the switch and port numbers to associate with the corresponding trunk. Note: You can configure two to four switch ports together as members of a trunk to a maximum of six trunks. Switch ports can only be assigned a member of a single trunk. There are no default settings.
	STP Learning	(1) Normal (2) Fast (3) Disabled	Choose the parameter that allows the specified trunk to participate in the spanning tree. This setting overrides those of the individual trunk members. Selecting Fast shortens the state transition timer by two seconds. The default setting is Normal.
	Trunk Mode	Basic	The default operating mode of the switch. When in Basic mode, source MAC addresses are dynamically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
	Trunk Name	1..20	Type a character string to create a unique name to identify the trunk, for example, Trunk1. The name, if chosen carefully, can provide meaningful information to you. For example, S1:T1 to FS2 indicates that Trunk1, in Switch1 connects to File Server 2.
MultiLink Trunk Group Setting	Trunk Status	(1) Enabled (2) Disabled	Choose to enable or disable any of the existing MultiLink Trunks. Note: When a trunk is not active (Trunk Status field set to Disabled), configuration changes do not take effect until you set the Trunk Status field to enabled.

2 Type information in the text boxes, or select from a list.

3 Click Submit in any section to save your changes.

Monitoring MLT traffic

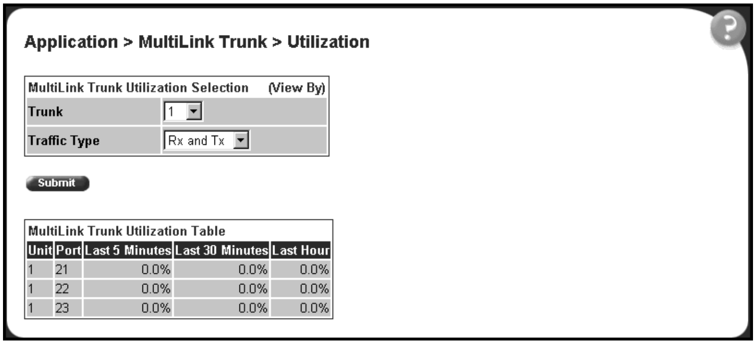
You can monitor the bandwidth usage for the MultiLink Trunk member ports within each trunk in your configuration by selecting the traffic type to monitor.

To monitor MultiLink Trunk traffic:

1 From the main menu, choose Application > MultiLink Trunk > Utilization.

The Utilization page opens (Figure 89).

Figure 89 Utilization page



Application > MultiLink Trunk > Utilization

MultiLink Trunk Utilization Selection	(View By)
Trunk	1
Traffic Type	Rx and Tx

MultiLink Trunk Utilization Table

Unit	Port	Last 5 Minutes	Last 30 Minutes	Last Hour
1	21	0.0%	0.0%	0.0%
1	22	0.0%	0.0%	0.0%
1	23	0.0%	0.0%	0.0%

Table 74 describes the items on the Utilization page.

Table 74 Utilization page items

Section	Item	Range	Description
MultiLink Trunk Utilization Selection (View By)	Trunk	1..6	Choose the trunk to be monitored.
	Traffic Type	(1) RX and TX (2) RX (3) TX	Choose the traffic type to be monitored for percentage of bandwidth utilization.

Table 74 Utilization page items (continued)

Section	**Item**	**Range**	**Description**
MultiLink Trunk Utilization Table	Unit/Port		A list of the trunk member switch ports that correspond to the trunk specified in the Trunk column.
	Last 5 Minutes%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last five minutes. This field provides a running average of network activity, and is updated every 15 seconds.
	Last 30 Minutes%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 30 minutes. This field provides a running average of network activity, and is updated every 15 seconds.
	Last Hour%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 60 minutes. This field provides a running average of network activity, and is updated every 15 seconds.

2 In the MultiLink Trunk Utilization Selection section, type the Trunk number and traffic type to be monitored.

3 Click Submit.

The results of your request are displayed in the MultiLink Trunk Utilization Table (Figure 89).

Chapter 8
Implementing Quality of Service (QoS)

You can configure Quality of Service (QoS) features in your network using the Web-based QoS Wizard or by using the advanced QoS configuration pages available in the Web-based management user interface. Refer to *Using the Business Policy Switch 2000 Software Version 1.2.* for a sample QoS configuration using the advanced QoS Web pages.

The configuration options discussed in this chapter are:

- "Using QoS Wizard," next
- "Configuring an interface group" on page 204
- "Configuring 802.1p priority queue assignment" on page 210
- "Configuring 802.1p priority mapping" on page 212
- "Creating a DSCP queue assignment" on page 213
- "Configuring DSCP mapping" on page 215
- "IP filter and IP filter group configurations" on page 217
- "Layer 2 filter and layer 2 filter group configurations" on page 227
- "Configuring QoS actions" on page 237
- "Configuring QoS meters" on page 241
- "Configuring QoS policies" on page 244
- "Configuring QoS Policy Agent (QPA) characteristics" on page 248

Note: To configure the software version 1.2 features in a mixed stack, you must access a BPS 2000 unit.

Using QoS Wizard

The QoS application delivers a set of tools that, when optimally configured, combats escalating bandwidth costs and optimizes application performance in your network.

QoS tools allow you to prioritize your critical applications and sensitive traffic. You can tailor appropriate services to support this traffic over the wide area, thus maintaining the necessary performance levels on an end-to-end basis.

You can configure QoS in your network with the Web-based management user interface using the “wizard” option or the detailed QoS pages.

The QoS Wizard automates the definition of common QoS settings for the BPS 2000. It features:

- Automatic generation of common QoS filters
- Optimal configuration of real time applications, for example, VoIP and streaming video

Warning: Nortel Networks recommends that you use the QoS Wizard for your *initial* configuration only. Each time the QoS Wizard is initiated, all existing configurations are reset to the default values. After you complete the *initial* QoS Wizard configuration method, you can then customize traffic treatment using the QoS Advanced configuration process.

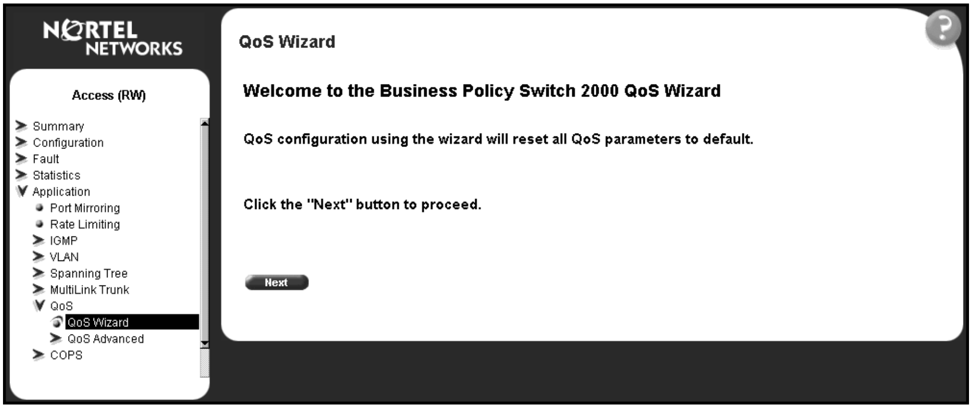
Configuring Standard traffic with the QoS Wizard

To use the QoS Wizard to configure Standard traffic:

1. From the main menu, choose Application > QoS > QoS Wizard.

   The QoS Wizard opens (Figure 90).

Figure 90 QoS Wizard opening page


NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
IGMP
VLAN
Spanning Tree
MultiLink Trunk
QoS
QoS Wizard
QoS Advanced
COPS
Next

QoS Wizard

Welcome to the Business Policy Switch 2000 QoS Wizard

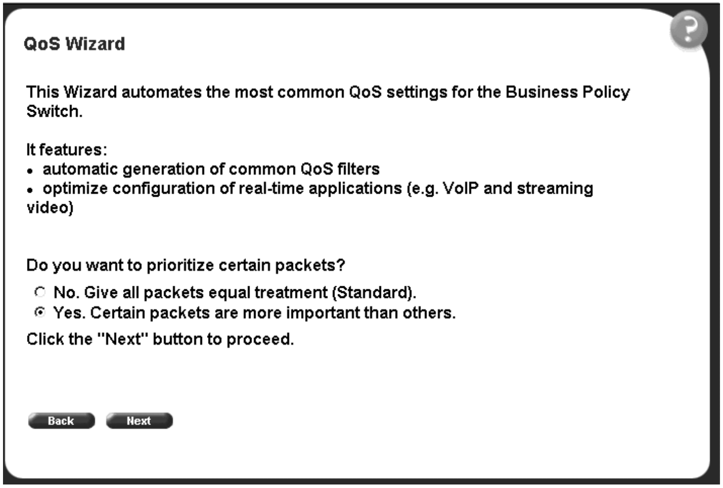
QoS configuration using the wizard will reset all QoS parameters to default.

Click the "Next" button to proceed.

2 To continue the configuration process, click Next.

A packet prioritization selection page opens (Figure 91).

Figure 91 Packet prioritization selection page



QoS Wizard

This Wizard automates the most common QoS settings for the Business Policy Switch.

It features:
- automatic generation of common QoS filters
- optimize configuration of real-time applications (e.g. VoIP and streaming video)

Do you want to prioritize certain packets?

○ No. Give all packets equal treatment (Standard).
● Yes. Certain packets are more important than others.

Click the "Next" button to proceed.

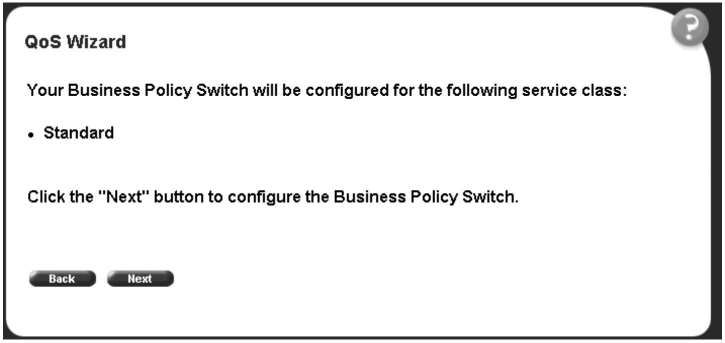
3 Select No.

4 Click Next.

A Standard prioritization page opens (Figure 92).

→ **Note:** If you want to prioritize traffic, skip this step and continue the steps outlined in "Prioritizing traffic with the QoS Wizard."

Figure 92 Standard prioritization page



QoS Wizard

Your Business Policy Switch will be configured for the following service class:

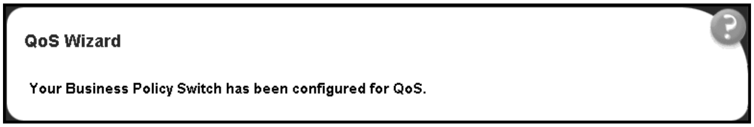
- Standard

Click the "Next" button to configure the Business Policy Switch.

5 To complete the configuration process, click Next.

The session confirmation page appears (Figure 93).

Figure 93 Session confirmation page



QoS Wizard

Your Business Policy Switch has been configured for QoS.

Prioritizing traffic with the QoS Wizard

You can specify that different types of traffic in your network configuration be marked with different priority levels.

To assign priority levels to different types of network traffic:

1 From the main menu, choose Application > QoS > QoS Wizard.

The QoS Wizard opens (Figure 90).

2 To continue the configuration process, click Next.

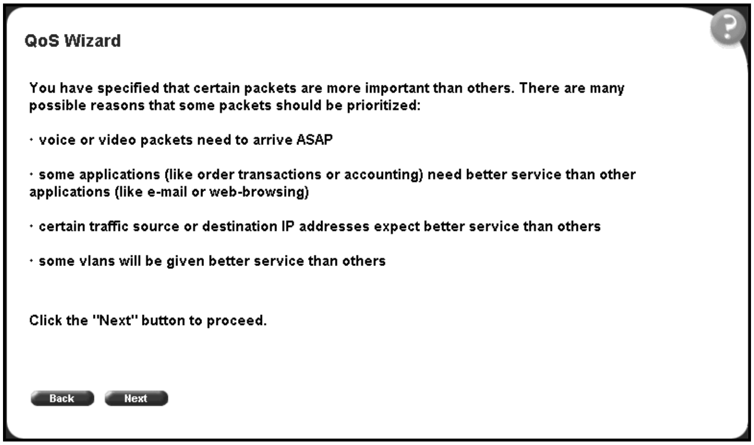
A packet prioritization selection page opens (Figure 91 on page 193).

3 Select Yes.

4 Click Next.

A packet prioritization explanation page opens (Figure 94).

Figure 94 Packet prioritization explanation page



QoS Wizard

You have specified that certain packets are more important than others. There are many possible reasons that some packets should be prioritized:

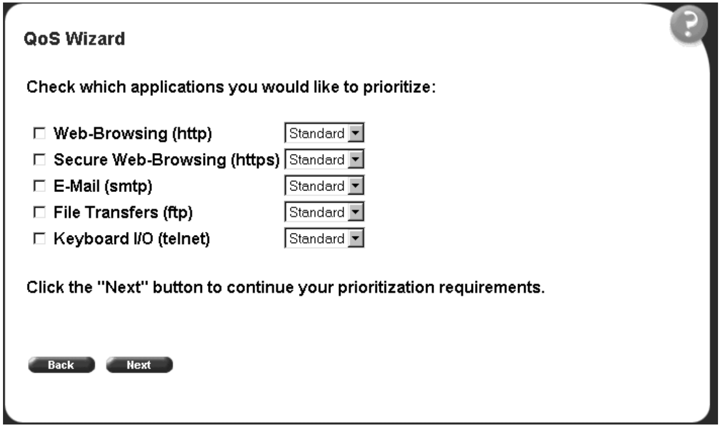
- voice or video packets need to arrive ASAP
- some applications (like order transactions or accounting) need better service than other applications (like e-mail or web-browsing)
- certain traffic source or destination IP addresses expect better service than others
- some vlans will be given better service than others

Click the "Next" button to proceed.

5 To continue the configuration process, click Next.

An application prioritization selection page opens (Figure 95).

Figure 95 Application prioritization selection page



QoS Wizard

Check which applications you would like to prioritize:

☐ Web-Browsing (http) Standard
☐ Secure Web-Browsing (https) Standard
☐ E-Mail (smtp) Standard
☐ File Transfers (ftp) Standard
☐ Keyboard I/O (telnet) Standard

Click the "Next" button to continue your prioritization requirements.

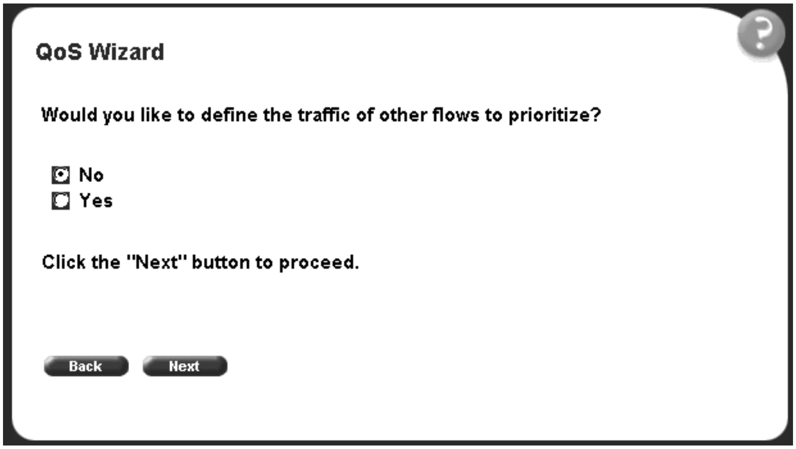
6 To choose an application for traffic prioritization, select the check box in the row of the application(s) you want.

7 From the list in each application row, choose the type of traffic prioritization you want.

8 Click Next.

An additional traffic flow prioritization page opens (Figure 96).

Figure 96 Additional traffic flow prioritization page



QoS Wizard

Would you like to define the traffic of other flows to prioritize?

● No
○ Yes

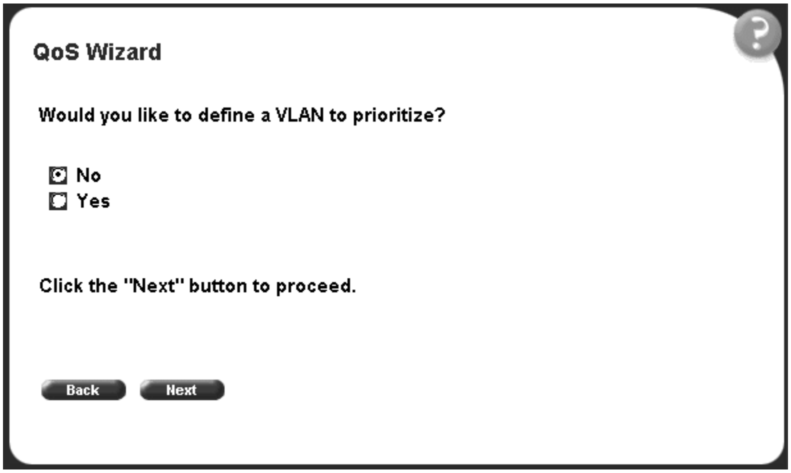
Click the "Next" button to proceed.

9 To complete the traffic prioritization session, select No.

10 Click Next.

A VLAN prioritization page opens (Figure 97).

Figure 97 VLAN prioritization page



QoS Wizard

Would you like to define a VLAN to prioritize?

● No
○ Yes

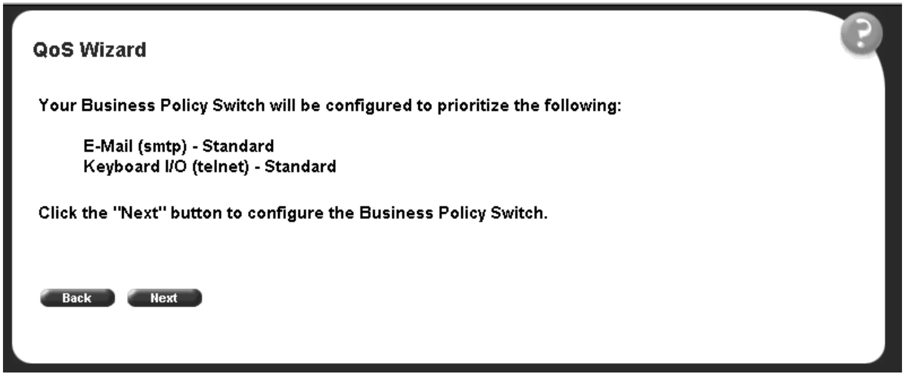
Click the "Next" button to proceed.

11 Select No.

12 Click Next.

A session verification page opens (Figure 98).

Figure 98 Session verification page



QoS Wizard

Your Business Policy Switch will be configured to prioritize the following:

E-Mail (smtp) - Standard
Keyboard I/O (telnet) - Standard

Click the "Next" button to configure the Business Policy Switch.

13 After verifying the information, click Next (or click Back to make changes to the appropriate pages).

A session confirmation page opens (Figure 93).

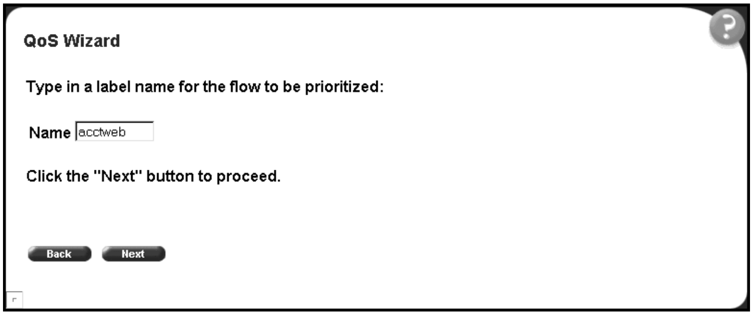
To configure additional traffic flows:

1 To define additional traffic flows, on the additional traffic flow priority page (Figure 96), select Yes.

2 Click Next.

A traffic flow label page opens (Figure 99).

Figure 99 Traffic flow label page



QoS Wizard

Type in a label name for the flow to be prioritized:

Name acctweb

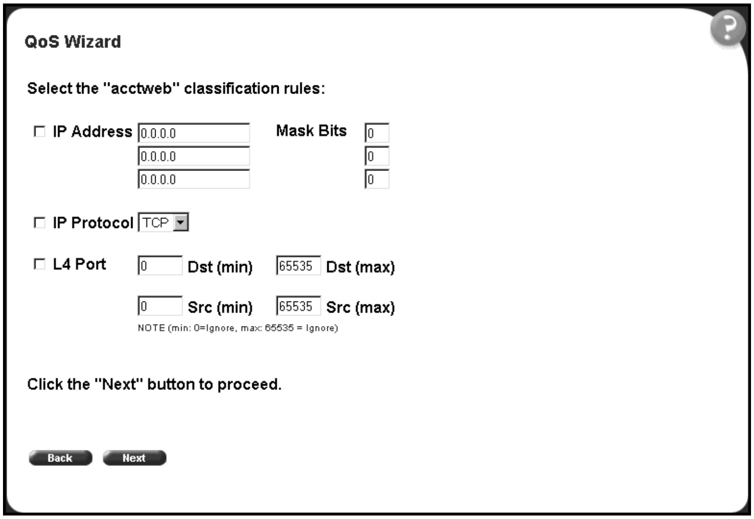
Click the "Next" button to proceed.

3 Type a character string to identify the traffic flow.

4 Click Next.

A classification rules page opens (Figure 100).

Figure 100 Classification rules page



QoS Wizard

Select the "acctweb" classification rules:

☐ IP Address 0.0.0.0 Mask Bits 0
0.0.0.0 0
0.0.0.0 0

☐ IP Protocol TCP

☐ L4 Port 0 Dst (min) 65535 Dst (max)

0 Src (min) 65535 Src (max)

NOTE (min: 0=Ignore, max: 65535 = Ignore)

Click the "Next" button to proceed.

Table 75 describes the items on the classification rules page.

Table 75 Classification rules page items

Item	Range	Description
IP Address	XXX.XXX.XXX.XXX	Select the check box to activate the classification rule, and then type the IP address to match against the packet’s source or destination IP address.
Mask Bits	Integer	Select the check box to activate the classification rule. Enter the number of left-justified mask bits for matching the source IP or destination address.
IP Protocol	TCP UDP	Select the check box to activate the classification rule, and then choose the IP protocol to match against the packet’s IP protocol field.
L4 Port Dst (min)	Integer (0.65535)	Select the check box to activate the classification rule, and then type the minimum value that the packet’s layer 4 destination port number must have and match this filter.
L4 Port Dst (max)	Integer (0.65535)	Select the check box to activate the classification rule, and then type the maximum value that the packet’s layer 4 destination port number must have and match this filter.

Table 75 Classification rules page items (continued)

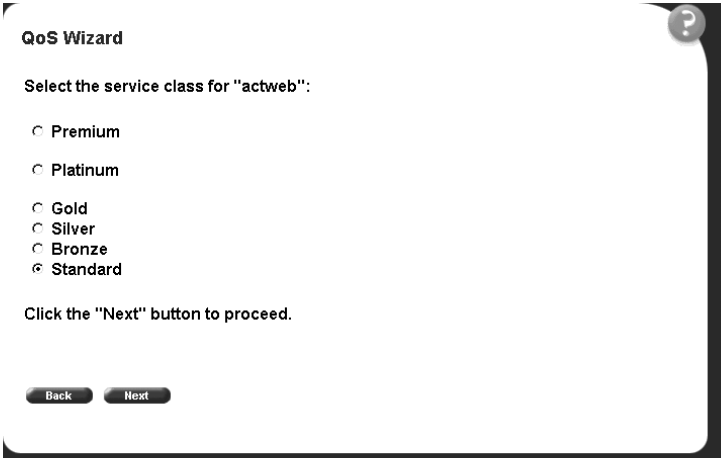
Item	Range	Description
L4 Port Src (min)	Integer (0.65535)	Select the check box to activate the classification rule, and then type the minimum value that the packet's layer 4 source port number must have and match this filter.
L4 Port Src (max)	Integer (0.65535)	Select the check box to activate the classification rule, and then type the maximum value that the packet's layer 4 source port number must have and match this filter.

5 Select the check box to activate the classification rule, and then type the appropriate information in the text boxes, or select from a list.

6 Click Next.

A service class assignment page opens (Figure 101).

Figure 101 Service class assignment page



QoS Wizard

Select the service class for "actweb":

○ Premium

○ Platinum

○ Gold
○ Silver
○ Bronze
● Standard

Click the "Next" button to proceed.

7 Select the check box of the priority level (service class) to assign to the traffic flow.

8. Click Next.

   An additional traffic prioritization page opens (Figure 96).

9. To define additional traffic flows, select Yes and repeat steps 1through 7; or select No.
10. Click Next.

    A VLAN prioritization page opens.

11. Select No.
12. Click Next.

    A session verification page opens (Figure 98).

13. After verifying the information, click Next (or click Back to make changes to the appropriate pages).

    A session confirmation page opens (Figure 93).

Prioritizing VLANs with the QoS Wizard

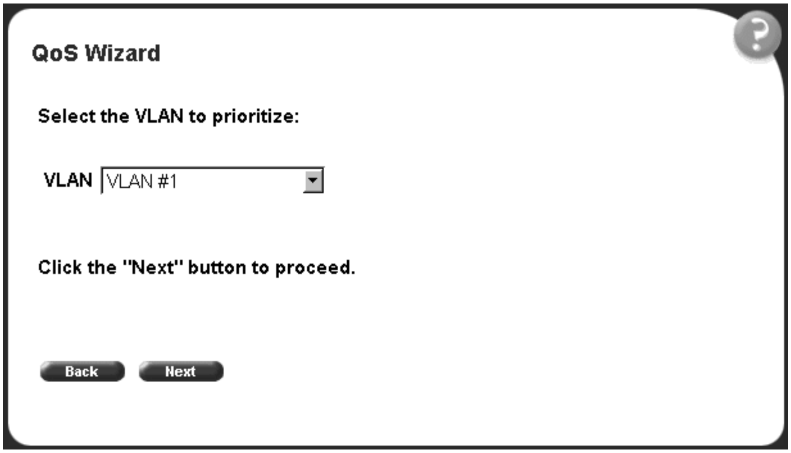
You can configure one VLAN to receive better service than others.

To configure a VLAN's priority:

1. On the VLAN prioritization page (Figure 97), select Yes.
2. Click Next.

   A VLAN selection page opens (Figure 102).

Figure 102 VLAN selection page



QoS Wizard

Select the VLAN to prioritize:

VLAN: VLAN #1

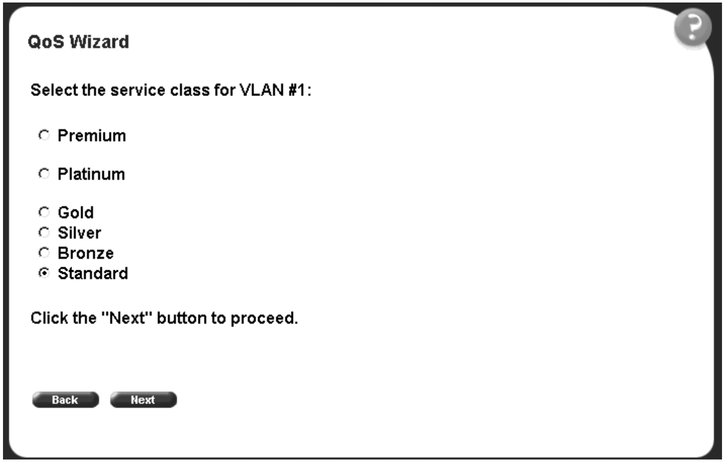
Click the "Next" button to proceed.

3 From the list, select the VLAN to receive better service.

4 Click Next.

A VLAN service class selection page opens (Figure 103).

Figure 103 VLAN service class selection page



QoS Wizard

Select the service class for VLAN #1:

- ○ Premium
- ○ Platinum
- ○ Gold
- ○ Silver
- ○ Bronze
- ● Standard

Click the "Next" button to proceed.

5 Select the check box of the priority level (service class) to assign to the VLAN.

6 Click Next.

A session verification page opens (Figure 98).

7 After verifying the information, click Next (or click Back to make changes to the appropriate pages).

A session confirmation page opens (Figure 93).

The number of applications you can select and the number of traffic flows you can define are dependent on the Business Policy Switch configuration environment. Refer to Table 76 for a list of filter limitations.

Table 76 QoS Wizard filter limitations

MDA/Configuration	Predefined applications (5 maximum)	User-defined flows (3 maximum)	VLAN (1 maximum)
No Gigabit MDAs/Business Policy Switch only	5	2	1
	4	3	1
	3	3	1
	2	3	1
	1	3	1
	0	3	1
No Gigabit MDAs/mixed stack	5	0	1
	4	0	1
	3	0	1
	2	1	1
	1	2	1
	0	3	1
Gigabit/Business Policy Switch only	5	0	1
	4	0	1
	3	0	1
	2	1	1
	1	2	1
	0	3	1
Gigabit/mixed stack	3	0	1
	2	0	1
	1	0	1
	0	2	1

Note: An extended sample of using the QoS Advanced pages to configure QoS parameters is shown in the *Using the Business Policy Switch 2000 Software Version 1.2*.

Configuring an interface group

You view existing interface group configurations, or create or modify an interface group if you want a port (or ports) to assign the same QoS policy to all interfaces in the group.

Note: One default role combination covers all ports of the device.

Creating an interface group configuration

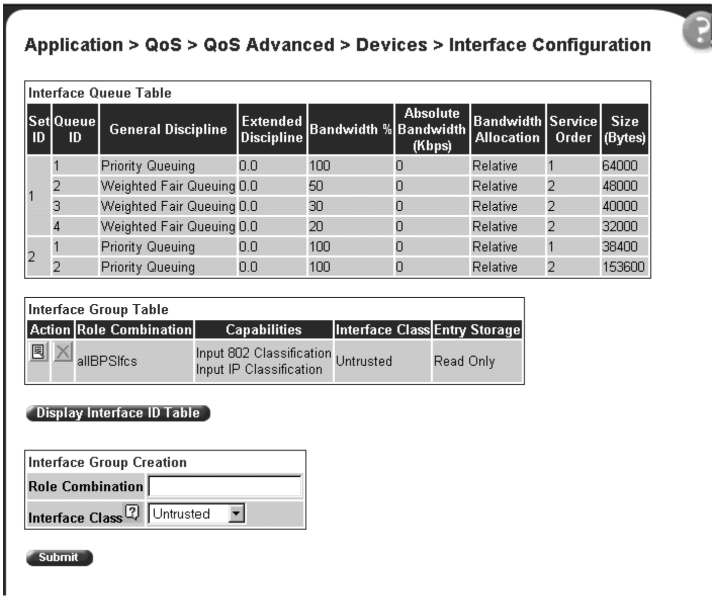
Note: For more information on QoS interface groups, or role combinations, refer to *Using the Business Policy Switch 2000 Software Version 1.2*.

To create an interface group configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

   The Interface Configuration page opens (Figure 104).

Figure 104 Interface Configuration page



Application > QoS > QoS Advanced > Devices > Interface Configuration

Interface Queue Table

Set ID	Queue ID	General Discipline	Extended Discipline	Bandwidth %	Absolute Bandwidth (Kbps)	Bandwidth Allocation	Service Order	Size (Bytes)
1	1	Priority Queuing	0.0	100	0	Relative	1	64000
	2	Weighted Fair Queuing	0.0	50	0	Relative	2	48000
	3	Weighted Fair Queuing	0.0	30	0	Relative	2	40000
	4	Weighted Fair Queuing	0.0	20	0	Relative	2	32000
2	1	Priority Queuing	0.0	100	0	Relative	1	38400
	2	Priority Queuing	0.0	100	0	Relative	2	153600

Interface Group Table

Action	Role Combination	Capabilities	Interface Class	Entry Storage
✎ ✕	allBPSIfcs	Input 802 Classification Input IP Classification	Untrusted	Read Only

Interface Group Creation

Role Combination	
Interface Class	Untrusted

Table 77 describes the items on the Interface Queue Table section of the Interface Configuration page.

Table 77 QoS Interface Queue Table section items

Item	Description
Set ID	The number that identifies a specific queue set.
Queue ID	The number that identifies the queue in the given set.
General Discipline	The queueing discipline that is associated with the specified queue. The options are: (1) Other - Use gosIfQueueExtDiscipline, (2) fifo - First In First Out Queuing, (3) pq -Priority Queuing, (4) fg - Fair Queuing, and (5) wfq - Weighted Fair Queuing
Extended Discipline	The queueing discipline that is associated with the specified queue. This attribute provides a means to add additional queueing mechanisms.
Bandwidth	The percentage of available bandwidth consumable to service the queue in one cycle.
Absolute Bandwidth	The absolute bandwidth consumable to service the queue in one cycle.
Bandwidth Allocation	Displays whether absolute or relative bandwidth is specified.
Service Order	The order in which a queue is serviced based on the defined discipline.
Size	The maximum size of the queue in bytes.

Table 78 describes the items on the Interface Group Table section of the Interface Group page.

Table 78 Interface Group Table section items

Item	**Description**
📝	Opens a modification page.
✖	Deletes the row.
Role Combination	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance (string 1..64). These identifiers are used within a number of classes to logically identify a physical set of interfaces to which policy rules and actions are applied.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select which policies and configurations may be pushed to the Policy Enforcement Point (PEP). The options are: (0) Other, (1) InputIpClassification, (2) output Ip Classification, (3) input 802 Classification, (4) output 802 Classification, (5) single Queuing Discipline, and (6) hybrid Queuing Discipline.
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted, Untrusted, and Unrestricted. See also “Traffic Type” in Table 79.
Entry Storage	Specifies whether or not the interface group can be deleted.

Note: For more information on QoS interface classes—or trusted, untrusted, and unrestricted ports—refer to *Using the Business Policy Switch 2000 Software Version 1.2.*

Table 79 describes the items on the Interface Group Creation section of the Interface Group page.

Table 79 Interface Group Creation section page items

Item and MIB association	Range	Description
Role Combination (qosInterfaceTypeRoles)	1..64	Type a character string to identify the role combination.
Interface Class (qosInterfaceTypeExtIfClass)	(1) Trusted (2) Untrusted (3) Unrestricted	Choose an interface class: Selecting Trusted requests the incoming DSCP value to not be changed, and instead be used for 802.1p user priority and queue assignment based on values in the DSCP mapping table and DSCP mapping table. Selecting Untrusted forces the incoming DSCP value (and associated mappings) to modify to a standard value by default. Actions associated with untrusted interfaces must re-mark the DSCP. Selecting Unrestricted allows you to configure actions that: • re-mark the DSCP or leave the DSCP as is • re-mark the 802.1p priority value or leave as is

2 In the Interface Group Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new interface group configuration appears in the Interface Group Table (Figure 104)

Displaying Interface ID Table

To display the Interface ID Table:

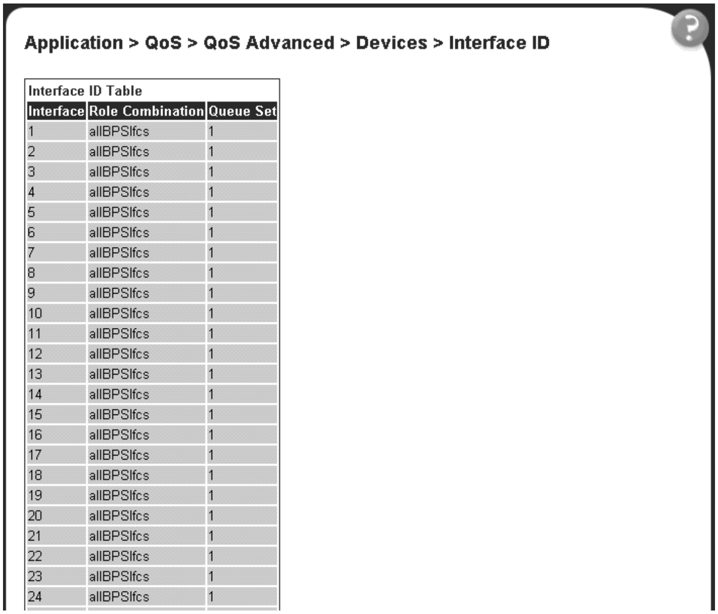
1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

The Interface Configuration page opens (Figure 104).

2 Click Display Interface ID Table.

The Interface ID page opens (Figure 105).

Figure 105 Interface ID page



Application > QoS > QoS Advanced > Devices > Interface ID

Interface ID Table

Interface	Role Combination	Queue Set
1	allBPSIfcs	1
2	allBPSIfcs	1
3	allBPSIfcs	1
4	allBPSIfcs	1
5	allBPSIfcs	1
6	allBPSIfcs	1
7	allBPSIfcs	1
8	allBPSIfcs	1
9	allBPSIfcs	1
10	allBPSIfcs	1
11	allBPSIfcs	1
12	allBPSIfcs	1
13	allBPSIfcs	1
14	allBPSIfcs	1
15	allBPSIfcs	1
16	allBPSIfcs	1
17	allBPSIfcs	1
18	allBPSIfcs	1
19	allBPSIfcs	1
20	allBPSIfcs	1
21	allBPSIfcs	1
22	allBPSIfcs	1
23	allBPSIfcs	1
24	allBPSIfcs	1

Table 81 describes the items on the Interface ID page.

Table 80 Interface ID page items

Item	Description
Interface	Displays the unit and port number.
Role Combination	Displays the role combination associated with the interface.
Queue Sets	Displays the queue set associated with this interface.

Adding or removing interface group members

To select or deselect ports as members of an existing interface group:

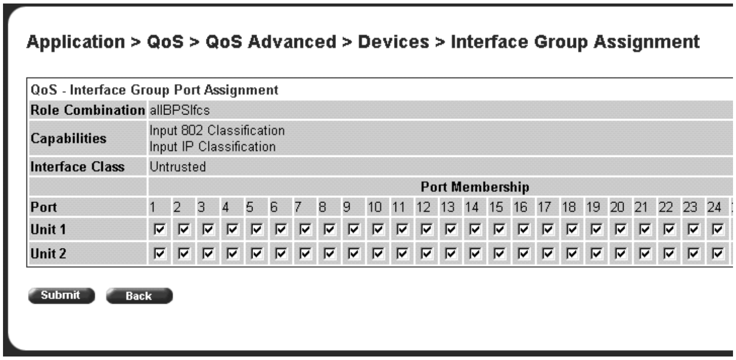
1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

The Interface Configuration page opens (Figure 104).

2 In the Interface Group Table section, in the row of your choice, click the Modify icon.

The Interface Group Assignment page opens (Figure 106).

Figure 106 Interface Group Assignment page



Application > QoS > QoS Advanced > Devices > Interface Group Assignment

QoS - Interface Group Port Assignment	
Role Combination	allBPSIfcs
Capabilities	Input 802 Classification Input IP Classification
Interface Class	Untrusted

	Port Membership																							
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Unit 2	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Table 81 describes the items on the Interface Group Assignment page.

Table 81 Interface Group Assignment page items

Item	Description
Role Combination	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance (string 1..64). These identifiers are used within a number of classes to logically identify a physical set of interfaces to which policy rules and actions are applied. This is the group of interfaces (interface group) to which policy rules and actions are applied.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select which policies and configurations may be pushed to the Policy Enforcement Point (PEP). The options are: (0) Other, (1) Input Ip Classification, (2) output Ip Classification, (3) input 802 Classification, (4) output 802 Classification, (5) single Queuing Discipline, and (6) hybrid Queuing Discipline
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted, Untrusted, and Unrestricted. See also "Traffic Type" in Table 79.
Port Membership	Select the external ports to associate with the interface group.
Cascade Ports	The cascade (internal) ports to associate with the interface group.

3 In the Port Membership section, click the check boxes of the ports to associate with the interface group.

4 Do one of the following:

- Click Submit.
- Click Back to return to the Interface Configuration page without making changes.

Deleting an interface group configuration

To delete an Interface group configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

   The Interface Configuration page opens (Figure 104).

2. In the Interface Group Table section, in the interface group configuration row of your choice, click the Modify icon.

   The Interface Group Assignment page opens (Figure 106).

3. In the Port Membership section, click the check boxes to deselect all ports associated with the interface group.
4. Click Submit.

   The Interface Configuration page is displayed (Figure 104).

5. In the Interface Group Table section, in the configuration row of your choice, click the Delete icon.

   A message opens prompting you to confirm your request.

6. Do one of the following:
   - Click Yes to delete the interface group configuration.
   - Click Cancel to return to the Interface Configuration page without making changes.

Configuring 802.1p priority queue assignment

Note: Nortel Networks recommends using the default 802.1p assignments to ensure end-to-end QoS connectivity.

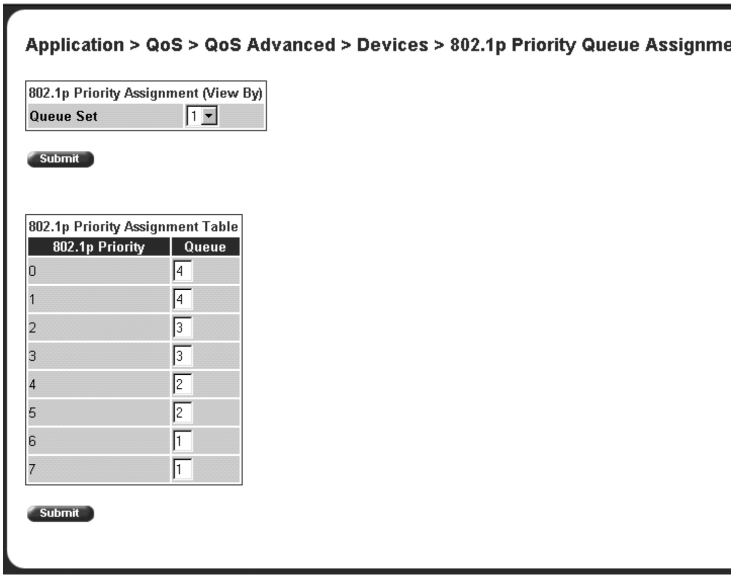
You can assign 802.1p user priority values to a queue for each interface with a specific queue set. This information is used for assigning egress traffic to outbound queues.

To configure 802.1p user priority:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Priority Q Assign.

The 802.1p Priority Queue Assignment page opens (Figure 107).

Figure 107 802.1p Priority Queue Assignment page



Application > QoS > QoS Advanced > Devices > 802.1p Priority Queue Assignme

802.1p Priority Assignment (View By)	
Queue Set	1

802.1p Priority Assignment Table

802.1p Priority	Queue
0	4
1	4
2	3
3	3
4	2
5	2
6	1
7	1

Table 82 describes the items on the 802.1p Priority Queue Assignment page.

Table 82 802.1p Priority Assignment Table section page items

Section	Item and MIB association	Description
802.1p Priority Assignment (View By)	Queue Set	Choose the queue set you want to modify.
802.1p Priority Assignment Table	802.1p Priority (ntnQosIfPriAssignmentPri)	The 802.1p user priority mapped to a queue.
	Queue (ntnQosIfPriAssignmentQueuet)	Type a number that signifies the desired queue in the specified queue set with which this priority is associated.

2 In the 802.1p Priority Assignment section, select the queue set to view in the 802.1p Priority Assignment Table.

3 Click Submit

The table is updated with the queue set you requested.

4 In the 802.1p Priority Assignment Table section, type the information in the text boxes.

5 Click Submit.

Note: Clicking Submit in the 802.1p Priority Assignment Table section results in a system reset.

Configuring 802.1p priority mapping

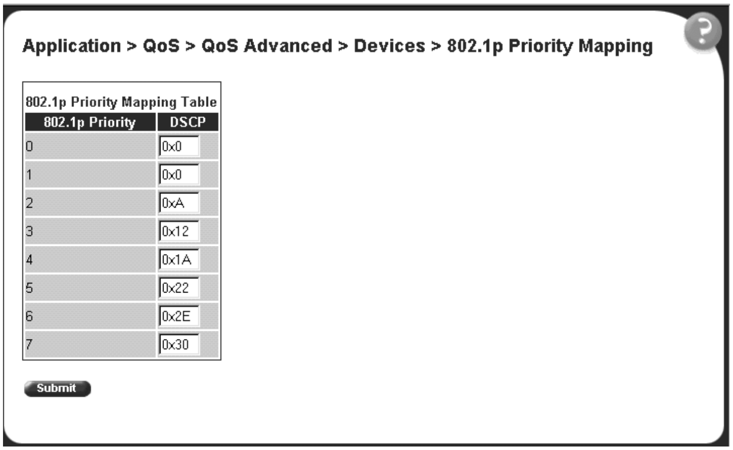
Note: Nortel Networks recommends using the default 802.1p priority to DSCP mappings to ensure end-to-end QoS connectivity.

To configure 802.1p priority to DSCP mapping:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Priority Mapping.

The 802.1p Priority Mapping page opens (Figure 108).

Figure 108 802.1p Priority Mapping page



Application > QoS > QoS Advanced > Devices > 802.1p Priority Mapping

802.1p Priority Mapping Table

802.1p Priority	DSCP
0	0x0
1	0x0
2	0xA
3	0x12
4	0x1A
5	0x22
6	0x2E
7	0x30

Table 83 describes the items on the 802.1p Priority Mapping page.

Table 83 802.1p Priority Mapping page items

Item	Description
802.1p Priority	The 802.1p user priority to map to a DSCP value at ingress.
DSCP	Type the DSCP value to associate with the specified 802.1p user priority value at ingress.

2 Type the information in the text boxes.

3 Click Submit.

Creating a DSCP queue assignment

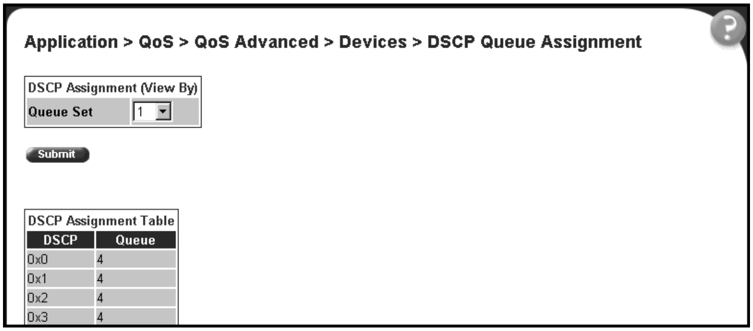
Note: Nortel Networks recommends using the default DSCP to queue set mappings to ensure end-to-end QoS connectivity.

To create a DSCP/queue set association:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > DSCP Q Assignment.

The DSCP Queue Assignment page opens (Figure 109).

Figure 109 DSCP Queue Assignment page


Application > QoS > QoS Advanced > Devices > DSCP Queue Assignment
Submit

DSCP Assignment (View By)

Queue Set 1

DSCP Assignment Table

DSCP	Queue
0x0	4
0x1	4
0x2	4
0x3	4

Table 84 describes the items on the DSCP Queue Assignment page.

Table 84 DSCP Queue Assignment page items

Section	Item	Format
DSCP Assignment (View By)	Queue Set	Choose the queue set to display in the DSCP Assignment Table.
DSCP Assignment Table	DSCP	The DSCP value to map to a queue.
	Queue	The queue set to which the traffic with the given DSCP value is associated.

2 In the DSCP Assignment (View By) section, choose the queue set to display in the DSCP Assignment Table.

The table is updated with information for the selected queue.

3 In the DSCP Assignment Table section, type the information in the text boxes.

4 Click Submit.

Configuring DSCP mapping

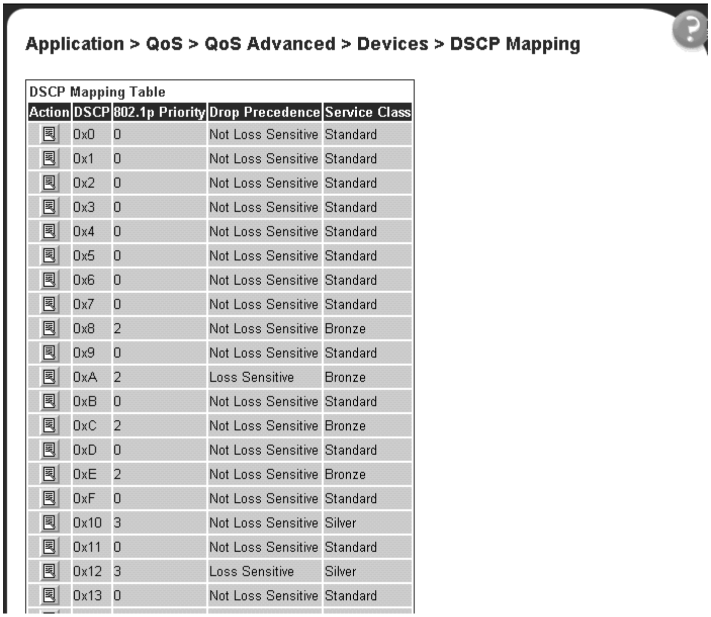
Note: Nortel Networks recommends using the default DSCP mappings to ensure end-to-end QoS connectivity.

To configure DSCP to 802.1p user priority/drop precedence mapping:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > DSCP Mapping.

The DSCP Mapping page opens (Figure 110).

Figure 110 DSCP Mapping Table page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Table

Action	DSCP	802.1p Priority	Drop Precedence	Service Class
▤	0x0	0	Not Loss Sensitive	Standard
▤	0x1	0	Not Loss Sensitive	Standard
▤	0x2	0	Not Loss Sensitive	Standard
▤	0x3	0	Not Loss Sensitive	Standard
▤	0x4	0	Not Loss Sensitive	Standard
▤	0x5	0	Not Loss Sensitive	Standard
▤	0x6	0	Not Loss Sensitive	Standard
▤	0x7	0	Not Loss Sensitive	Standard
▤	0x8	2	Not Loss Sensitive	Bronze
▤	0x9	0	Not Loss Sensitive	Standard
▤	0xA	2	Loss Sensitive	Bronze
▤	0xB	0	Not Loss Sensitive	Standard
▤	0xC	2	Not Loss Sensitive	Bronze
▤	0xD	0	Not Loss Sensitive	Standard
▤	0xE	2	Not Loss Sensitive	Bronze
▤	0xF	0	Not Loss Sensitive	Standard
▤	0x10	3	Not Loss Sensitive	Silver
▤	0x11	0	Not Loss Sensitive	Standard
▤	0x12	3	Loss Sensitive	Silver
▤	0x13	0	Not Loss Sensitive	Standard

Table 85 describes the items on the DSCP Mapping Table page.

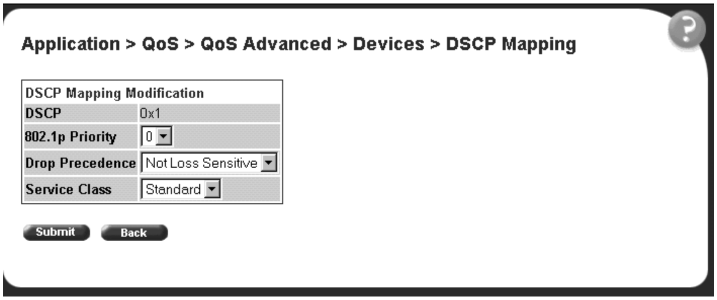
Table 85 DSCP Mapping Table page items

Item	Format
📝	Opens a modification page.
DSCP	The attribute used internally to determine the appropriate Layer 2 cost of service (CoS) mappings.
802.1p Priority	The IEEE802 CoS value used when mapping the DSCP value specified by the qos802DscpMappingDscp attribute to an IEEE 802 CoS.
Drop Precedence	The drop value precedence used for traffic with the associated 802.1D user priority value with the identified queue. Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	The current service class. The options are: 1) Premium, (2) Platinum, (3) Gold, (4) Silver, (5) Bronze, (6) Standard, (7) Network, and (8) Critical. Note: This field corresponds to the adjacent user priority levels.

2 In the row of your choice, click the Modification icon.

The DSCP Mapping Modification page opens (Figure 111).

Figure 111 DSCP Mapping Modification page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Modification	
DSCP	0x1
802.1p Priority	0
Drop Precedence	Not Loss Sensitive
Service Class	Standard

Table 86 describes the items on the DSCP Mapping Modification page.

Table 86 DSCP Mapping Modification page items

Item	Range	Format
DSCP	0..63	Type the attribute to use internally to determine the appropriate Layer 2 cost of service (CoS) mappings.
802.1p Priority	0..7	Choose the IEEE802 CoS value to use when mapping the DSCP value specified by the qos802DscpMappingDscp attribute to an IEEE 802 CoS.

Table 86 DSCP Mapping Modification page items (continued)

Item	Range	Format
Drop Precedence	Loss Sensitive Not Loss Sensitive	Choose the drop value precedence to use for traffic with the associated 802.1p user priority value with the identified queue. Selecting a Loss Sensitive value specifies a low packet drop precedence; selecting a Not Loss Sensitive value specifies a high packet drop precedence. Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	(1) Premium (2) Platinum (3) Gold (4) Silver (5) Bronze (6) Standard (7) Network (8) Critical	Choose the service class. Note: This field corresponds to the adjacent user priority levels.
	Note: Mappings created on the DSCP mapping modification page are used at egress for marking traffic: • Trusted and unrestricted IP traffic—If you select the re-marking action of using the egress map, the mappings determine the 802.1p priority and drop precedence values associated with packets based on the DSCP of the received packet. • Untrusted and untresticted traffic—If you select the re-marking action of using default, the mappings determine the 802.1p priority and drop precedence values associated with packets based on the DSCP value you specified in the Update DSCP action field.	

3 Select from a list.

4 Click Submit.

The modified configuration appears in the DSCP Mapping Table (Figure 110).

Note: For more information on QoS interface classes—or trusted, untrusted, and unrestricted ports—refer to *Using the Business Policy Switch 2000 Software Version 1.2*.

IP filter and IP filter group configurations

You can create an IP filter, which enables the switch to classify traffic. In turn, you can create an access control list from a series of defined filters to create an IP filter group. The filter group then determines access to and denial of network services.

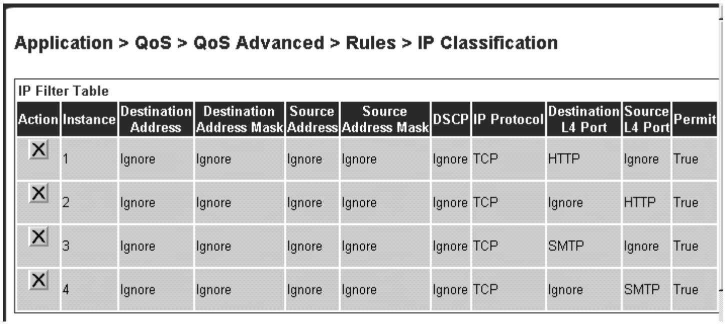
Creating an IP filter configuration

To create an IP filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 112, Figure 113, and Figure 114).

Figure 112 IP Classification page (1 of 3)

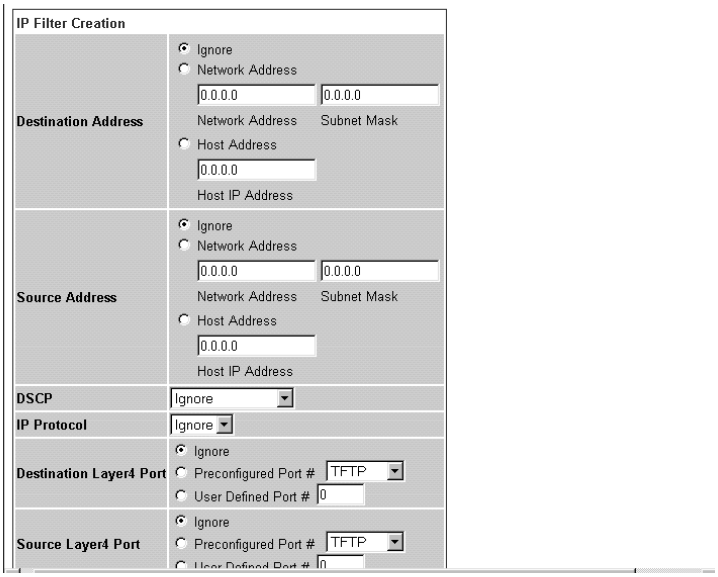


Application > QoS > QoS Advanced > Rules > IP Classification

IP Filter Table

Action	Instance	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	IP Protocol	Destination L4 Port	Source L4 Port	Permit
☒	1	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	HTTP	Ignore	True
☒	2	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	HTTP	True
☒	3	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	SMTP	Ignore	True
☒	4	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	SMTP	True

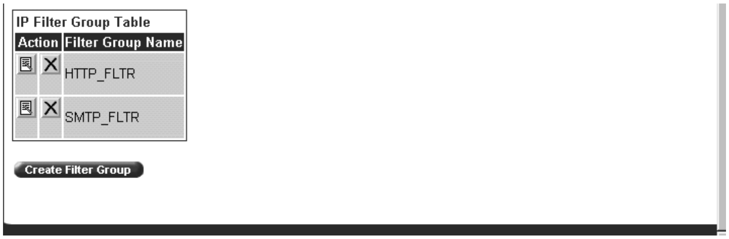
Figure 113 IP Classification page (2 of 3)



IP Filter Creation

Destination Address	● Ignore ○ Network Address 0.0.0.0 (Network Address) 0.0.0.0 (Subnet Mask) ○ Host Address 0.0.0.0 (Host IP Address)
Source Address	● Ignore ○ Network Address 0.0.0.0 (Network Address) 0.0.0.0 (Subnet Mask) ○ Host Address 0.0.0.0 (Host IP Address)
DSCP	Ignore ▾
IP Protocol	Ignore ▾
Destination Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ▾ ○ User Defined Port # 0
Source Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ▾ ○ User Defined Port # 0

Figure 114 IP Classification page (3 of 3)



IP Filter Group Table

Action	Filter Group Name
🗎 ✕	HTTP_FLTR
🗎 ✕	SMTP_FLTR

Note: When you choose the Ignore value, the filter matches all criteria for that parameter.

Table 87 describes the items on the IP Filter Table and IP Filter Creation sections of the IP Classification page.

Table 87 IP Filter Table and Filter Creation sections page items

Section	**Item and MIB association**	**Range**	**Description**
IP Filter Table	Action	☒	Deletes the row. Note: You cannot delete a filter if it is referenced in a filter group.
	Instance		Displays unique identifier.
	Destination Address (qosIpAceDstAddr)	XXX.XXX.XXX.XXX	Displays the IP address to match against the packet's destination IP address.
	Destination Address Mask (qosIpAceDstAddrMask)	XXX.XXX.XXX.XXX	Displays the mask for the matching of the destination IP address. A zero bit in the mask means that the corresponding bit in the address always matches. One (1) bits must be left justified.
	Source Address (qosIpAceSrcAddr)	XXX.XXX.XXX.XXX	Displays the IP address to match against the packet's source IP address.
	Source Address Mask (qosIpAceSrcAddrMask)	XXX.XXX.XXX.XXX	Displays the mask for the matching of the source IP address. One (1) bits must be left justified.
	DSCP (qosIpAceDscp)	Ignore, Integer (0..63)	Displays the value that the DSCP in the packet must have and match this filter. This displays the DSCP value that this filter attempts to match.
	Protocol (qosIpAceProtocol)	TCP (6) UDP (17) ICMP (1) IGMP (2) RSVP (46) Ignore (0)	Displays the IP protocol to match against the packet's IP protocol field.
	Destination L4 Port (qosIpAceDstL4PortMin) (qosIpAceDstL4PortMax)	Integer (0.65535)	Displays the value that the packet's layer 4 destination port number must have and match this filter.
	Source L4 Port (qosIpAceSrcL4PortMin) (qosIpAceSrcL4PortMax)	Integer (0.65535)	Displays the value that the packet's layer 4 source port number must have and match this filter.
	Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
IP Filter Creation/ Destination Address	Ignore		Click if you want the filter to ignore the packet's destination IP address.
	Network Address	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's destination network address. Enter the IP address to match against the packet's destination IP address.
	Subnet Mask)	XXX.XXX.XXX.XXX	Enter the mask for the matching of the destination IP address. A zero bit in the mask means that the corresponding bit in the address always matches. One (1) bits must be left justified.

Table 87 IP Filter Table and Filter Creation sections page items (continued)

Section	Item and MIB association	Range	Description
	Host Address)	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's destination host IP address. Enter the IP address to match against the packet's destination IP address.
IP Filter Creation/ Source Address	Ignore		Click if you want the filter to ignore the packet's source IP address.
	Network Address	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's source network address. Enter the IP address to match against the packet's source IP address.
	Subnet Mask)	XXX.XXX.XXX.XXX	Enter the mask for the matching of the source IP address. One (1) bits must be left justified.
	Host Address)	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's source host IP address. Enter the IP address to match against the packet's source IP address.
IP Filter Creation/ DSCP	DSCP (qosIpAceDscp)	Ignore, Integer (0..63)	Choose the value that the DSCP in the packet must have and match this filter.
IP Filter Creation/ IP Protocol	Protocol (qosIpAceProtocol)	Ignore (0) TCP (6) UDP (17) ICMP (1) IGMP (2) RSVP (46)	Choose the IP protocol to match against the packet's IP protocol field.
IP Filter Creation/ Destination Layer4 Port	Ignore		Click if you want the filter to ignore the packet's layer 4 destination port.
	Preconfigured Port #	TFTP FTP TELNET SMTP HTTP HTTPS	Choose the value that the packet's layer 4 destination port number must have and match this filter.
	User Defined Port #	Integer	Enter the value that the packet's layer 4 destination port number must have and match this filter.
IP Filter Creation/ Source Layer4 Port	Ignore		Click if you want the filter to ignore the packet's layer 4 source port.
	Preconfigured Port #	TFTP FTP TELNET SMTP HTTP HTTPS	Choose the value that the packet's layer 4 source port number must have and match this filter.
	User Defined Port #	Integer	Enter the value that the packet's layer 4 source port number must have and match this filter.

2 In the IP Filter Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new IP filter configuration appears in the IP Filter Table (Figure 112).

Note: An IP filter configuration is not modifiable. The filter must be deleted and then re-created.

Deleting an IP filter configuration

To delete an IP filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 122).

2 In the IP Filter Table, in the IP filter configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the IP filter configuration.
- Click Cancel to return to the IP Classification page without making changes.

Note: You cannot delete a filter if it is referenced in a filter group.

Creating an IP filter group configuration

To create an IP filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 112).

Table 88 describes the items on the IP Filter Group section of the IP Classification page.

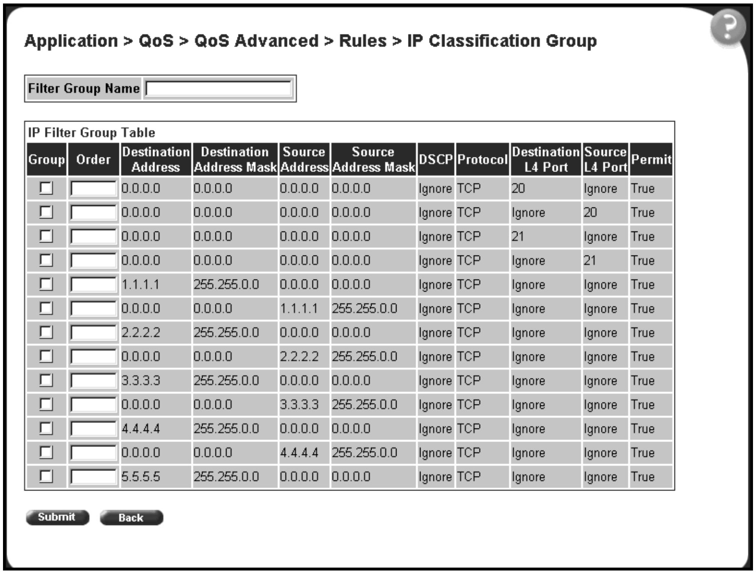
Table 88 IP Filter Group section page items

Item	Description
📝	Opens a modification page.
✖	Deletes the row.
Filter Group Name	A list of existing filter group configurations.
Create Filter Group	Opens a filter group creation page.

2 Click Create Filter Group.

The IP Classification Group page opens (Figure 115).

Figure 115 IP Classification Group page



Application > QoS > QoS Advanced > Rules > IP Classification Group

Filter Group Name

IP Filter Group Table

Group	Order	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Port	Permit
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	20	Ignore	True
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	20	True
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	21	Ignore	True
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	21	True
☐		1.1.1.1	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	1.1.1.1	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		2.2.2.2	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	2.2.2.2	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		3.3.3.3	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	3.3.3.3	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		4.4.4.4	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	4.4.4.4	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		5.5.5.5	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True

Table 89 describes the items on the IP Classification Group page.

Table 89 IP Classification Group page items

Item	**Range**	**Description**
Filter Group Name	1..16	Enter a character string to create an identity for the filter group configuration.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Type a number to establish the evaluation order of filters in the group.
Destination Address		The IP address that is matched against the packet's destination IP address.
Destination Address Mask		The mask for the matching of the destination IP address. Note: A zero bit in the mask means that the corresponding bit in the address always matches.
Source Address		The IP address that is matched against the packet's source IP address.
Source Address Mask		The mask for the matching of the source IP address.
DSCP		The value that the DSCP in the packet must have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP
Destination L4 Port		The value that the packet's layer 4 destination port number can have and match the filter entry.
Source L4 Port		The value that the packet's layer 4 source port number can have and match the filter entry.
Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3 Type information in the text boxes, or click the check box.

4 Click Submit.

The new configuration appears in the IP Filter Group Table (Figure 112).

Modifying an IP filter group configuration

To modify an IP filter group configuration:

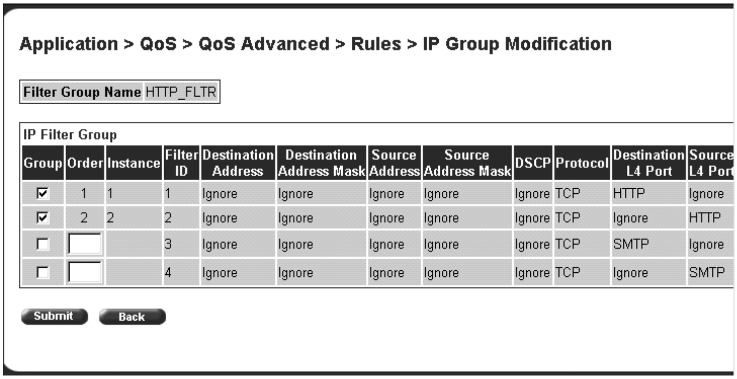
1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 112).

2 In the IP Filter Group Table section, in the IP filter group configuration of your choice, click the Modify icon.

The IP Group Modification page opens (Figure 116).

Figure 116 IP Group Modification page



Application > QoS > QoS Advanced > Rules > IP Group Modification

Filter Group Name HTTP_FLTR

IP Filter Group

Group	Order	Instance	Filter ID	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Por
☑	1	1	1	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	HTTP	Ignore
☑	2	2	2	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	HTTP
☐	☐		3	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	SMTP	Ignore
☐	☐		4	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	SMTP

Table 90 describes the items on the IP Group Modification page.

Table 90 IP Modification Group page items

Item	Range	Description
Filter Group Name	1..16	Displays the name of the selected the filter group.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Displays the order for existing groups. Enter the desired order for the entries you are adding to the group.
Instance		Displays unique identifier.
Filter ID		Displays the filter identifier.
Destination Address		The IP address that is matched against the packet's destination IP address.
Destination Address Mask		The mask for the matching of the destination IP address. Note: A zero bit in the mask means that the corresponding bit in the address always matches.
Source Address		The IP address that is matched against the packet's source IP address.
Source Address Mask		The mask for the matching of the source IP address.
DSCP		The value that the DSCP in the packet must have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP
Destination L4 Port		The value that the packet's layer 4 destination port number can have and match the filter entry.

Table 90 IP Modification Group page items

Item	**Range**	**Description**
Source L4 Port		The value that the packet's layer 4 source port number can have and match the filter entry.
Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3. Select (or deselect) the filter as a member of the Filter Group.
4. Click Submit.

Deleting an IP filter group configuration

To delete an IP filter group configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

   The IP Classification page opens (Figure 112).

2. In the IP Filter Group Table section, in the IP filter group configuration row of your choice, click the Delete icon.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the IP filter group configuration.
   - Click Cancel to return to the IP Classification page without making changes.

Note: You cannot delete a filter group that is referenced by a policy. You must first delete the policy.

Layer 2 filter and layer 2 filter group configurations

You can configure layer 2 filters by defining IEEE 802-based parameters, and selective layer 3 and layer 4 parameters. Layer 2 filter groups are defined by specifying the layer 2 filter to be included in the given filter group.

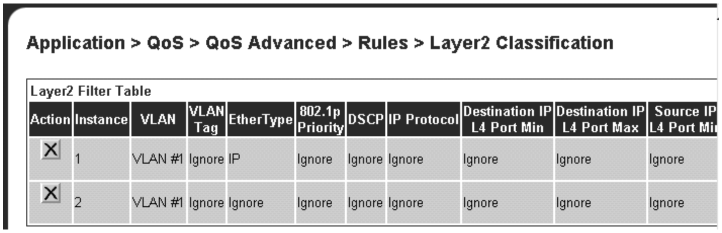
Creating a layer 2 filter configuration

To create a layer2 filter configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

   The Layer2 Classification page opens (Figure 117, Figure 118, and Figure 119).

Figure 117 Layer2 Classification page (1 of 3)

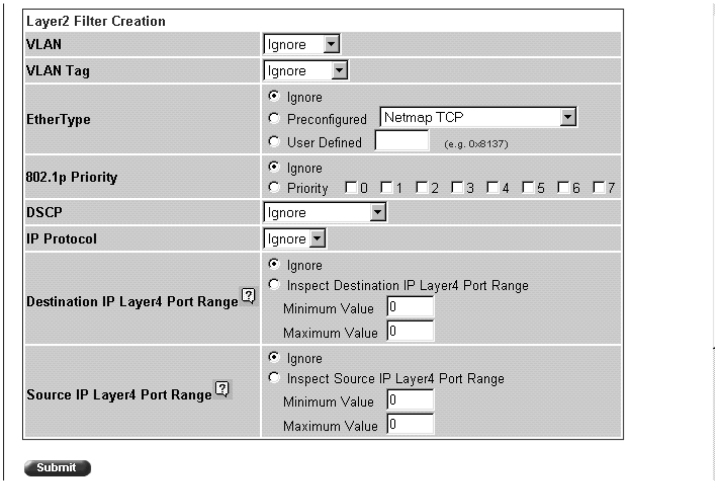


Application > QoS > QoS Advanced > Rules > Layer2 Classification

Layer2 Filter Table

Action	Instance	VLAN	VLAN Tag	EtherType	802.1p Priority	DSCP	IP Protocol	Destination IP L4 Port Min	Destination IP L4 Port Max	Source IP L4 Port Mi
☒	1	VLAN #1	Ignore	IP	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore
☒	2	VLAN #1	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore

Figure 118 Layer2 Classification page (2 of 3)



Layer2 Filter Creation

VLAN: Ignore

VLAN Tag: Ignore

EtherType: ● Ignore ○ Preconfigured Netmap TCP ○ User Defined (e.g. 0x8137)

802.1p Priority: ● Ignore ○ Priority ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

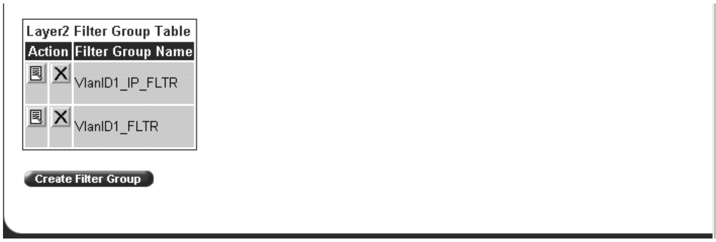
DSCP: Ignore

IP Protocol: Ignore

Destination IP Layer4 Port Range: ● Ignore ○ Inspect Destination IP Layer4 Port Range; Minimum Value 0; Maximum Value 0

Source IP Layer4 Port Range: ● Ignore ○ Inspect Source IP Layer4 Port Range; Minimum Value 0; Maximum Value 0

Figure 119 Layer2 Classification page (3 of 3)



Layer2 Filter Group Table

Action	Filter Group Name
	VlanID1_IP_FLTR
	VlanID1_FLTR

Table 91 describes the items on the Layer2 Filter Table and Layer2 Filter Creation sections of the Layer2 Classification page.

Table 91 Layer2 Filter Table and Layer2 Filter Creation section items

Section	Item	Range	Description
Layer 2 Filter Table	Action	☒	Deletes the row.
	Instance		Displays unique identifier.
	VLAN	Ignore, 1-4094	Displays the VLAN number.

Table 91 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	Item	Range	Description
	VLAN Tag	(1) Tagged (2) Untagged (3) Ignore	Displays whether or not to check VLAN tagging.
	EtherType	Ignore Netmap TCP Netmap XNS XTP LOOP Vines Vines IP Banyan Vines Echo Vines Banyan Echo ARP RARP IP IPv6 3Com NBP 3Com NBP Ack 3Com NBP ConnReq 3Com NBP ConnRsp 3Com NBP ConnComplt 3Com NBP CloseReq 3Com NBP CloseRsp 3Com NBP Datagram 3Com NBP Broadcast 3Com NBP NBP NameClaim 3Com NBP DelName LAP Atalk ARP Atalk IBM Net Mon IBMRT XNS Compatibility XNS IPX Netware SNMP User Defined	Displays the EtherType to match.
	802.1p Priority	Ignore, 0...7.	Displays the 802.1p priority level.
	DSCP	Ignore, Integer (0.63)	Displays the value that the DSCP in the packet must have and match this filter.

Table 91 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	Item	Range	Description
	IP Protocol	Ignore TCP UDP ICMP IGMP RSVP	Displays the IP protocol to match against the packet's IP protocol field.
	Destination IP L4 Port Min	Ignore, Integer (0.65535)	Displays the least value that the packet's layer 4 destination port number can have and match this filter.
	Destination IP L4 Port Max	Ignore, Integer (0.65535)	Displays the maximum value that the packet's layer 4 destination port number can have and match this filter.
	Source IP L4 Port Min	Ignore, Integer (0.65535)	Displays the least value that the packet's layer 4 source port number can have and match this filter.
	Source IP L4 Port Max	Ignore, Integer (0.65535)	Displays the maximum value that the packet's layer 4 source port number can have and match this filter.
Layer2 Filter Creation	VLAN	Ignore, 1-4094	Choose the VLAN name or ID number.
	VLAN Tag	(1) Tagged (2) Untagged (3) Ignore	Choose whether or not to check VLAN tagging.

Table 91 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	Item	Range	Description
	EtherType	Ignore Netmap TCP Netmap XNS XTP LOOP Vines Vines IP Banyan Vines Echo Vines Banyon Echo ARP RARP IP IPv6 3Com NBP 3Com NBP Ack 3Com NBP ConnReq 3Com NBP ConnRsp 3Com NBP ConnComplt 3Com NBP CloseReq 3Com NBP CloseRsp 3Com NBP Datagram 3Com NBP Broadcast 3Com NBP NBP NameClaim 3Com NBP DelName LAP Atalk ARP Atalk IBM Net Mon IBMRT XNS Compatibility XNS IPX Netware SNMP User Defined	Choose the EtherType to match. Note: If you choose User Defined, enter the value.
	802.1p Priority	Ignore, 0...7.	Click the 802.1p priority level.
	DSCP	Ignore, Integer (0..63)	Choose the value that the DSCP in the packet must have and match this filter.

Table 91 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	Item	Range	Description
	IP Protocol	Ignore TCP UDP ICMP IGMP RSVP	Select the IP protocol to match against the packet's IP protocol field.
	Destination IP L4 Port Range	Ignore, Min, Max	Choose Ignore or type the minimum value and the maximum value that the packet's layer 4 destination port number can have and match this filter.
	Source IP L4 Port Range	Ignore, Min, Max	Choose Ignore or type the minimum value and the maximum value that the packet's layer 4 source port number can have and match this filter.

2 Type the information in the text boxes, or select from a list.

3 Click Submit.

The new Layer2 filter configuration appears in the Layer2 Filter Table (Figure 117).

Note: You cannot delete a filter if it is referenced in a filter group.

Deleting a layer 2 filter configuration

To delete a layer 2 filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 117).

2 In the Layer2 Filter Table, in the layer 2 filter configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the filter configuration.
- Click Cancel to return to the Layer2 Classification page without making changes.

Note: A Layer 2 filter configuration cannot be modified. The configuration must be deleted and then recreated.

Creating a layer 2 filter group configuration

To create a Layer 2 filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 117).

Table 92 describes the items on the Layer2 Filter Group Table section of the Layer2 Classification page.

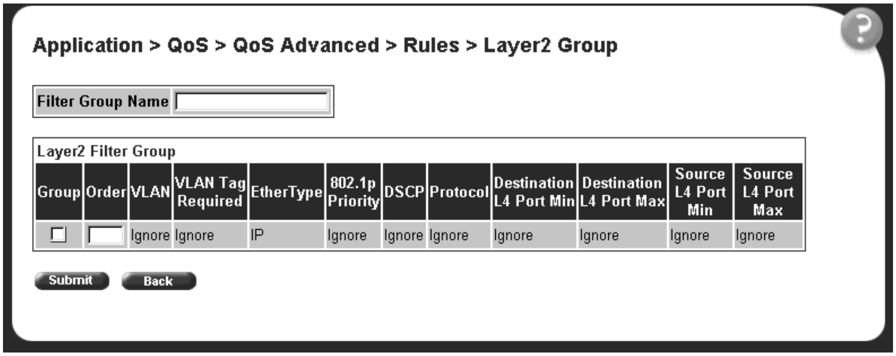
Table 92 IP Filter Group Table section items

Item	**Description**
📝	Opens a modification page.
✖	Deletes the row.
Filter Group Name	Lists existing filter group configurations.
Create Filter Group	Opens a filter group creation page.

2 Click Create Filter Group.

The Layer2 Group page opens (Figure 120).

Figure 120 Layer2 Group page



Application > QoS > QoS Advanced > Rules > Layer2 Group

Filter Group Name

Layer2 Filter Group

Group	Order	VLAN	VLAN Tag Required	EtherType	802.1p Priority	DSCP	Protocol	Destination L4 Port Min	Destination L4 Port Max	Source L4 Port Min	Source L4 Port Max
☐		Ignore	Ignore	IP	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore

Table 93 describes the items on the Layer2 Group page.

Table 93 Layer2 Group page items

Item	Range	Description
Filter Group Name	1..16	Enter a character string to create an identity for the filter group configuration.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Enter a number to establish the evaluation order of filters in the group.
VLAN		The VLAN ID specified when the layer 2 filter was created.
VLAN Tag Required		The VLAN tag requirement option selected when the filter was created.
EtherType		The EtherType selected when the filter was created.
802.1p Priority		The 802.1p priority selected when the filter was created.
DSCP		The value that the DSCP in the packet can have and match this filter.
Protocol		The IP protocol that is matched against the packet’s IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP.
Destination L4 Port Min		The least value that the packet’s layer 4 destination port number can have and match this filter.
Destination L4 Port Max		The maximum value that the packet’s layer 4 destination port number can have and match this filter.
Source L4 Port Min		The least value that the packet’s layer 4 source port number can have and match this filter.

Table 93 Layer2 Group page items

Item	Range	Description
Source L4 Port Max		The maximum value that the packet's layer 4 source port number can have and match this filter.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3 Type information in the text boxes, or click the check box.

4 Click Submit.

The new layer 2 filter group configuration appears in the Layer Filter Group Table (Figure 117).

Modifying a layer 2 filter group configuration

To modify a layer 2 filter group configuration:

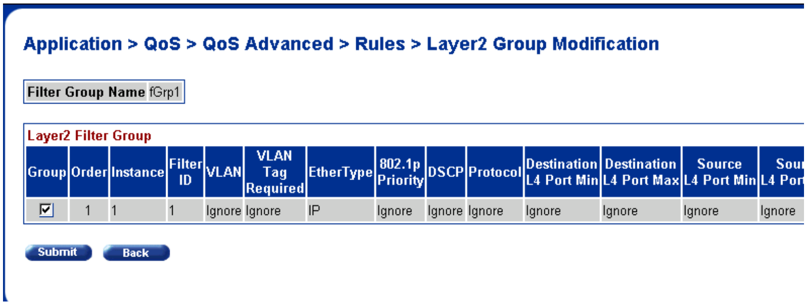
1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 117).

2 In the Layer2 Filter Group Table section, in the layer 2 filter group configuration of your choice, click the Modify icon.

The Layer2 Group modification page opens (Figure 121).

Figure 121 Layer2 Group modification page



Application > QoS > QoS Advanced > Rules > Layer2 Group Modification

Filter Group Name fGrp1

Layer2 Filter Group

Group	Order	Instance	Filter ID	VLAN	VLAN Tag Required	EtherType	802.1p Priority	DSCP	Protocol	Destination L4 Port Min	Destination L4 Port Max	Source L4 Port Min	Sou L4 Por
☑	1	1	1	Ignore	Ignore	IP	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore

Table 94 describes the items on the Layer2 Group modification page.

Table 94 Layer2 Group modification page items

Item	Range	Description
Filter Group Name	1..16	Displays the filter group name.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Enter a number to establish the evaluation order of filters in the group.
Instance		Displays a unique identifier.
Filter ID		Displays the filter identifier.
VLAN		The VLAN ID specified when the layer 2 filter was created.
VLAN Tag Required		The VLAN tag requirement option selected when the filter was created.
EtherType		The EtherType selected when the filter was created.
802.1p Priority		The 802.1p priority selected when the filter was created.
DSCP		The value that the DSCP in the packet can have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP.
Destination L4 Port Min		The least value that the packet's layer 4 destination port number can have and match this filter.
Destination L4 Port Max		The maximum value that the packet's layer 4 destination port number can have and match this filter.
Source L4 Port Min		The least value that the packet's layer 4 source port number can have and match this filter.
Source L4 Port Max		The maximum value that the packet's layer 4 source port number can have and match this filter.

3. Type information in the text boxes, or click the check box.
4. Click Submit.

Deleting a layer 2 filter group configuration

To delete a layer 2 filter group configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

   The Layer2 Classification page opens (Figure 117).

2. In the Layer2 Filter Group Table section, in the layer 2 filter group configuration row of your choice, click the Delete icon.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the filter group configuration.
   - Click Cancel to return to the Layer2 Classification page without making changes.

➡ **Note:** You cannot delete a filter group that is referenced by a policy. You must first delete the policy.

Configuring QoS actions

When you create a filter action, you specify the actions to be associated with specific IP and IEEE 802 filter groups. An action specifies the type of behavior you want a policy to apply to a flow of packets. When the filters match the incoming packets, the created actions are performed on those packets.

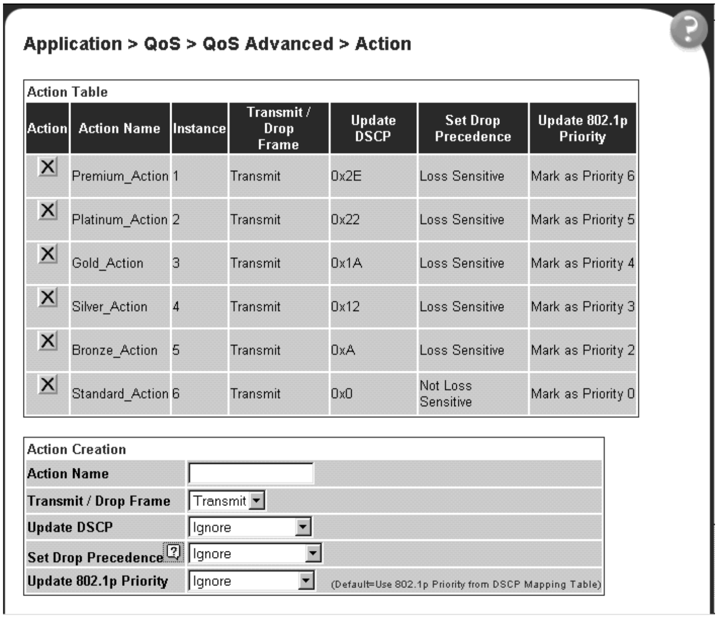
Creating a filter action configuration

To create a filter action configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Actions.

   The Action page opens (Figure 122).

Figure 122 Action page



Application > QoS > QoS Advanced > Action

Action Table

Action	Action Name	Instance	Transmit / Drop Frame	Update DSCP	Set Drop Precedence	Update 802.1p Priority
☒	Premium_Action	1	Transmit	0x2E	Loss Sensitive	Mark as Priority 6
☒	Platinum_Action	2	Transmit	0x22	Loss Sensitive	Mark as Priority 5
☒	Gold_Action	3	Transmit	0x1A	Loss Sensitive	Mark as Priority 4
☒	Silver_Action	4	Transmit	0x12	Loss Sensitive	Mark as Priority 3
☒	Bronze_Action	5	Transmit	0xA	Loss Sensitive	Mark as Priority 2
☒	Standard_Action	6	Transmit	0x0	Not Loss Sensitive	Mark as Priority 0

Action Creation

Action Name		
Transmit / Drop Frame	Transmit	
Update DSCP	Ignore	
Set Drop Precedence	Ignore	
Update 802.1p Priority	Ignore	(Default=Use 802.1p Priority from DSCP Mapping Table)

Table 95 describes the items on the Action page.

Table 95 Action page items

Item and MIB association	Range	Description
☒		Deletes the row.
Action Name	1..16	Type a character string to uniquely identify the action configuration.
Instance		Displays the unique identifier.
Transmit/Drop Frame (qosActionDrop)	(1) Transmit (2) Drop	Choose whether the frame being evaluated should be dropped or transmitted by this attribute. The default setting is Transmit.
Update DSCP (qosActionUpdateDSCP)	Ignore or integer	Type a value. When this field is defined, it causes the value contained in the Differentiated Services (DS) field of an associated IP datagram to be updated with the value of this object. The default setting is Ignore.

Table 95 Action page items (continued)

Item and MIB association	Range	Description
Set Drop Precedence (ntnQosActionExtSetDropPrec)	(1) Ignore (2) Loss Sensitive (3) Not loss Sensitive (4) Use Defaults (5) Use Egress Map	Choose a packet drop precedence value. Note: Generally, low packet drop precedence receives preferential treatment The default setting is Use Defaults
Update 802.1p Priority (ntnQosActionExtUpdatePri)	(1) Ignore (2) Priority 0 (3) Priority 1 (4) Priority 2 (5) Priority 3 (6) Priority 4 (7) Priority 5 (8) Priority 6 (9) Priority 7 (10) Use Defaults (11) Use Egress Map	Choose the action attribute that causes the value contained in the 802.1p priority field to be updated based on the value of this object. The update priority range values are 0 (lowest priority) to 7 (highest priority). Note: Use Defaults=Use 802.1p priority from DSCP mapping table. The default setting is Use Defaults.

2 In the Action Creation section, type information in the text boxes, or select from a list

3 Click Submit.

The new filter action configuration appears in the Action Table (Figure 122).

➡ **Note:** Actions are not modifiable. They must be deleted and re-created.

Creating In-Profile and Out-Profile actions

If you want to meter your data, you must create both an In-Profile action and an Out-Profile action. The In-Profile action directs the switch how to handle the data flow that is within the meter you set (refer to "Configuring QoS meters"), and the Out-Profile directs the switch how to handle all other data.

As you can create several meters, you can create several different in-profile and out-of-profile actions, for various traffic policing scenarios. Be sure to assign different names to the different action. Note that you must always create an in-profile action, even if you use non-metered data.

To create In-Profile and Out-Profile actions:

1. Create and name an In-Profile Action.
2. Create and name your own Out-Profile Action.
3. Click Submit

Deleting an action configuration

To delete an action configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Actions.

   The Action page opens (Figure 122).

2. In the Action Table section, in the filter action configuration row of your choice, click the Delete icon.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the filter configuration.
   - Click Cancel to return to the Action page without making changes.

Note: You cannot delete an action that is referenced by a meter. you must first delete the meter.

Configuring QoS meters

You must create meters when using the QoS Web-based management interface Advanced Pages. You choose either No Meter Data or Metered Data, which sets metering, or policing limits, on the traffic.

Note: You must create meters for every action.
If you do not want to meter the data, or police the data, choose No Meter Data. You need only create an In-Profile action for this type of data.
If you want to meter, or police, the data, choose Metered Data. You must create both In-Profile and Out-of-Profile actions for metered data.

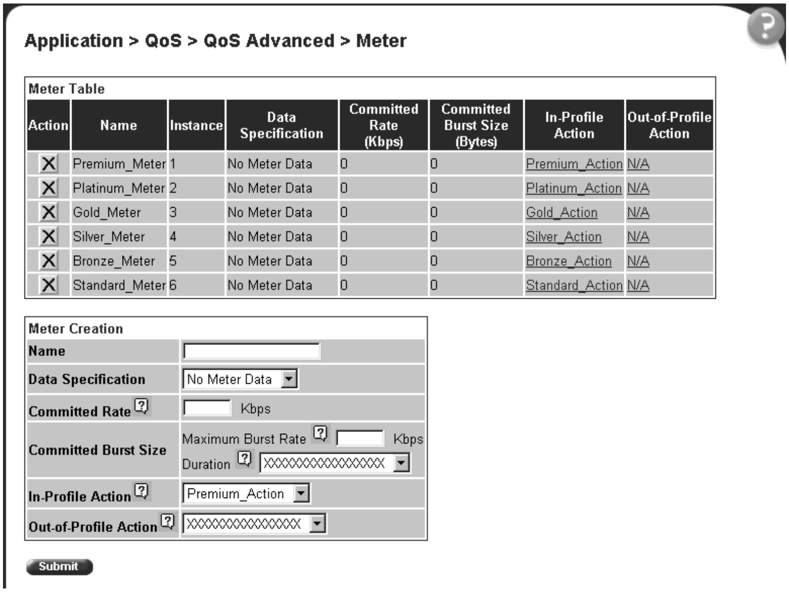
Creating a meter

To create a meter:

1 From the main menu, choose Application > QoS > QoS Advanced > Meters.

The Meter page opens (Figure 123).

Figure 123 Meter page



Application > QoS > QoS Advanced > Meter

Meter Table

Action	Name	Instance	Data Specification	Committed Rate (Kbps)	Committed Burst Size (Bytes)	In-Profile Action	Out-of-Profile Action
☒	Premium_Meter	1	No Meter Data	0	0	Premium_Action	N/A
☒	Platinum_Meter	2	No Meter Data	0	0	Platinum_Action	N/A
☒	Gold_Meter	3	No Meter Data	0	0	Gold_Action	N/A
☒	Silver_Meter	4	No Meter Data	0	0	Silver_Action	N/A
☒	Bronze_Meter	5	No Meter Data	0	0	Bronze_Action	N/A
☒	Standard_Meter	6	No Meter Data	0	0	Standard_Action	N/A

Meter Creation

Name	
Data Specification	No Meter Data
Committed Rate	Kbps
Committed Burst Size	Maximum Burst Rate Kbps Duration XXXXXXXXXXXXXXXX
In-Profile Action	Premium_Action
Out-of-Profile Action	XXXXXXXXXXXXXXXX

2 In the Meter Creation area, create the meters.

Table 96 describes the fields in the Meter Creation area, which you use to set new meters.

Table 96 Meter Creation fields

Item	Range	Description
Name	1 to 16 alphanumeric characters with no spaces	Enter the name for the meter you are creating.
Data Specification	(1) No Meter Data (2) Metered Data	Choose whether you want to meter the data or not. Note: When you choose No Meter Data, do not complete the Committed Rate, Committed Burst Size, or Out-Profile Action fields in the box.
Committed Rate	13 - 1,700,000 Kbps	Use this field ***only*** if you specified metered data for this filter (refer to Data Specification, above). Enter the Committed Rate in Kbps here.
Committed Burst Size	2,047 to 131,071 bytes 7 durations	Use this field ***only*** if you specified metered data for this filter (refer to Data Specification, above). Maximum Burst Rate—Enter the Maximum Burst Rate in bytes. Duration—From the pull-down menu, choose 1 of the 7 durations for the period that the Maximum Burst Rate is allowed.
In-Profile Action	Configured, user-defined actions	Choose the action you want for either: • No Meter data - Choose among 6 actions • In-Profile metered data - Choose among the In-Profile actions you previously configured using the Actions page
Out-Profile Action		Use this field ***only*** if you specified metered data for this filter (refer to Data Specification, above). Choose among the Out-Profile actions you previously configured using the Actions page.

3 Click Submit.

4 If you have not already specified the interface assignments, choose Applications > QoS > QoS Advanced > Devices > Interface Configuration page to connect the desired ports to the desired filters.

Note: Meter configurations are not modifiable. They must be deleted and the information re-entered.

Viewing meters

To view a meter:

1. From the main menu, choose Application > QoS > QoS Advanced > Meters.

   The Meters page opens (Figure 123).

2. View created meters in the Meter Table.

   Table 97 describes the fields in the Meter Table area.

Table 97 Meter Table fields

Item	Range	Description
Action	☒	Deletes the meter.
Name		Displays the name of the meter.
Instance		Displays the unique identifier.
Data Specification	(1) No Meter Data (2) Metered Data	Displays whether the meter has metered data or not.
Committed Rate	13 - 1,700,000 Kbps	Displays the Committed Rate in kbps.
Committed Burst Size	2,047 to 131,071 bytes	Displays the Committed Burst Size in bytes.
In-Profile Action	Configured, user-defined action	Displays the In-Profile Action for this meter.
Out-Profile Action	Configured, user-defined action	With a meter using metered data, this field displays the action specified for traffic that is out-of-profile. With a meter using no metered data, this field displays N/A.

Deleting a meter

To delete a meter:

1. From the main menu, choose Application > QoS > QoS Advanced > Meters.

   The Meter page opens (Figure 123).

2. In the Meter Table section, click the Delete icon to delete the meter.

   A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the meter configuration.
- Click Cancel to return to the Meter page without making changes.

➡ **Note:** You cannot delete a meter that is referenced by a policy. You must delete the policy first.

Configuring QoS policies

You can configure QoS policies by creating filters in the hardware that apply a set of packet filtering criteria and actions to individual interfaces.

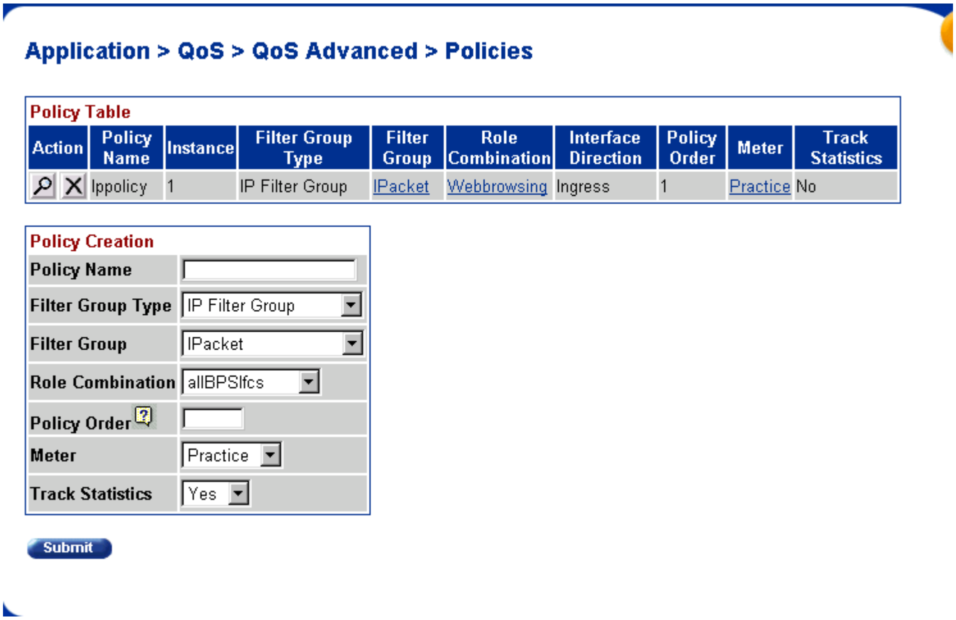
Installing defined filters

To create a hardware policy filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The Policies page opens (Figure 124).

Figure 124 Policies page



Application > QoS > QoS Advanced > Policies

Policy Table

Action	Policy Name	Instance	Filter Group Type	Filter Group	Role Combination	Interface Direction	Policy Order	Meter	Track Statistics
🔍 ✕	Ippolicy	1	IP Filter Group	IPacket	Webbrowsing	Ingress	1	Practice	No

Policy Creation

Policy Name	
Filter Group Type	IP Filter Group
Filter Group	IPacket
Role Combination	allBPSIfcs
Policy Order	
Meter	Practice
Track Statistics	Yes

Note: Policy configurations are not modifiable. They must be deleted and the information re-entered.

Table 98 describes the items on the Policy page.

Table 98 Policy page items

Section	Item and MIB association	Range	Description
Policy Table	Action	🔍	Opens a view only statistics table. The table displays current filter statistics in bytes and packets.
		✕	Deletes the row.
	Policy Name	1..16	A list of the names of existing target configurations.
	Instance		Displays the unique identifier.
	Filter Group Type		The type of filter group that is referenced by this instance of the Target class. The options are: IP Filter Group or Layer2 Filter Group.
	Filter Group		The filter group that is associated with this target.
	Role Combination		The interfaces to which this target specification applies, specified in terms of a role combination tag.
	Interface Direction		The direction of packet flow at the interface to which this target specification applies.
	Policy Order		The number used to determine the order of precedence for this target specification.
	Meter		The meter associated with this entry.
Policy Creation	Policy Name	1..64	Type a character string to create a unique name to identify this policy.
	Filter Group Type (qosTargetAclType)	(1) IP Filter Group (2) Layer2 Filter Group	Choose the type of filter group to associate with this policy.
	Filter Group		Choose the filter group to associate with this policy.
	Role Combination (qosTargetInterfaceRoles)		Choose the type of interface to which this policy applies, specified in terms of a role combination.
	Policy Order (qosTargetOrder)	Integer	Enter a number to use as a determinate of the order of precedence for this filter.
	Meter (qosTargetMeter)		Choose the metering action associated with this entry.
	Track Statistics (ntnQosTargetStatsTrack Statistics)	(1) Yes (2) No	Choose whether or not to track statistics for policy.

Viewing a hardware policy configuration

To view statistics for a selected hardware policy configuration:

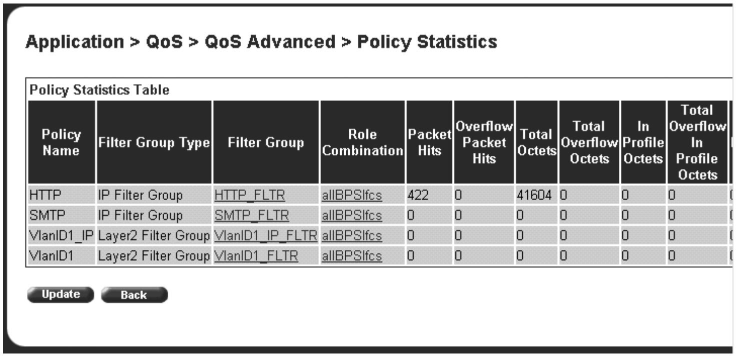
1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The Policies page opens (Figure 124).

2 In the Policy Table section, in the filter group configuration of your choice, click the View icon.

The Policy Statistics page opens (Figure 125).

Figure 125 Policy Statistics page



Application > QoS > QoS Advanced > Policy Statistics

Policy Statistics Table

Policy Name	Filter Group Type	Filter Group	Role Combination	Packet Hits	Overflow Packet Hits	Total Octets	Total Overflow Octets	In Profile Octets	Total Overflow In Profile Octets
HTTP	IP Filter Group	HTTP_FLTR	allBPSIfcs	422	0	41604	0	0	0
SMTP	IP Filter Group	SMTP_FLTR	allBPSIfcs	0	0	0	0	0	0
VlanID1_IP	Layer2 Filter Group	VlanID1_IP_FLTR	allBPSIfcs	0	0	0	0	0	0
VlanID1	Layer2 Filter Group	VlanID1_FLTR	allBPSIfcs	0	0	0	0	0	0

Table 99 describes the items on the Policy Statistics page.

Table 99 Policy Statistics page items

Item and MIB association	Description
Policy Name	The name of the selected policy.
Filter Group Type	The type of group that is referenced by this instance of the filter policy class. The options are: IP Filter Group or Layer2 Filter Group.
Filter Group	The filter group associated with the selected policy.
Role Combination	The interfaces to which this policy applies, specified in terms of a role combination.
Packet Hits	The packets selected for additional processing. The action taken is based on a match with specified filter and/or threshold information.
Overflow Packet Hits	The number of times the associated ntnQosTargetPktHits counter overflowed.
Total Octets	The total number of octets associated with packet hits for this policy.
Total Overflow Octets	The total number of times the associated ntnQosTargetTotalOctets counter overflowed.

Table 99 Policy Statistics page items (continued)

Item and MIB association	Description
In Profile Octets	The total number of in-profile octets associated with packet hits for this policy.
Total Overflow In Profile Octets (ntnQosTargetTotalInProfOctets)	The total number of times the associated ntnQosTargetTotalOctets counter overflowed.
Out Profile Octets	The total number of out-of-profile octets associated with packet hits for this policy.
Total Overflow Out Profile Octets (ntnQosTargetTotalOutProfOctets	The total number of times the associated ntnQosTargetTotalOctets counter overflowed.

3. To refresh the hardware policy statistics, click Update.

Deleting a hardware policy configuration

To delete a hardware policy configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Policies.

   The Policies page opens (Figure 124).

2. In the Policy Table section, in the hardware policy configuration row of your choice, click the Delete icon.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the hardware policy configuration.
   - Click Cancel to return to the Policy page without making changes.

Configuring QoS Policy Agent (QPA) characteristics

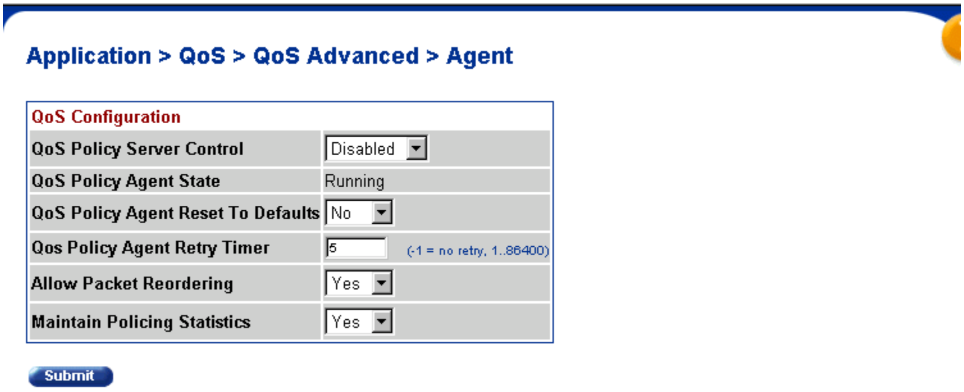
You can configure QPA operational parameters.

To open the Agent page:

1 From the main menu, choose Application > QoS > QoS Advanced > Agent.

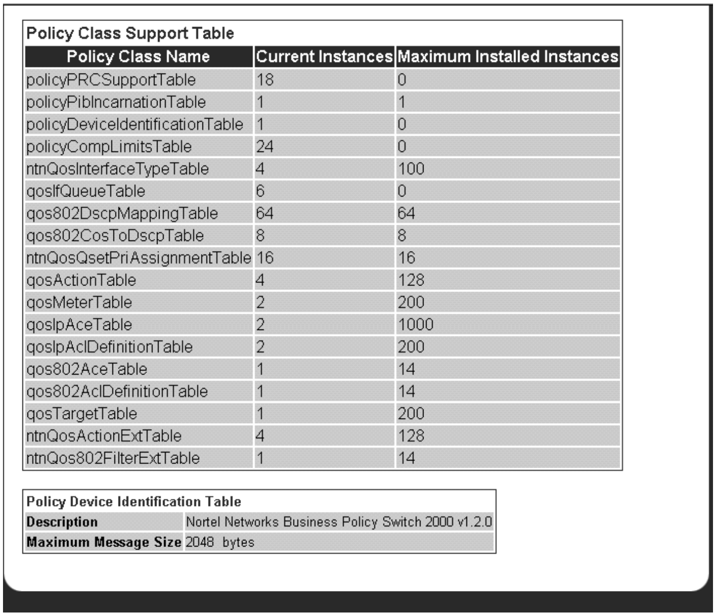
The Agent page opens (Figure 126 and Figure 127).

Figure 126 Agent page (1 of 2)



QoS Configuration	
QoS Policy Server Control	Disabled
QoS Policy Agent State	Running
QoS Policy Agent Reset To Defaults	No
Qos Policy Agent Retry Timer	5 (-1 = no retry, 1..86400)
Allow Packet Reordering	Yes
Maintain Policing Statistics	Yes

Figure 127 Agent page (2 of 2)



Policy Class Support Table

Policy Class Name	Current Instances	Maximum Installed Instances
policyPRCSupportTable	18	0
policyPibIncarnationTable	1	1
policyDeviceIdentificationTable	1	0
policyCompLimitsTable	24	0
ntnQosInterfaceTypeTable	4	100
qosIfQueueTable	6	0
qos802DscpMappingTable	64	64
qos802CosToDscpTable	8	8
ntnQosQsetPriAssignmentTable	16	16
qosActionTable	4	128
qosMeterTable	2	200
qosIpAceTable	2	1000
qosIpAclDefinitionTable	2	200
qos802AceTable	1	14
qos802AclDefinitionTable	1	14
qosTargetTable	1	200
ntnQosActionExtTable	4	128
ntnQos802FilterExtTable	1	14

Policy Device Identification Table

Description	Nortel Networks Business Policy Switch 2000 v1.2.0
Maximum Message Size	2048 bytes

Table 100 describes the items on the Agent page.

Table 100 Agent page items

Section	Item and MIB association	Range	Description
QoS Configuration	QoS Policy Server Control	Enabled Disabled	Choose to enable or disable the QoS Policy server control. Note: Choosing to enable COPS disables local policy control.
	QoS Policy Agent State (ntnQosConfigQpaState)	Running Initialized Disabled	The current status of the policy agent.
	QoS Policy Agent Reset to Defaults (ntnQosConfigQpaState)	(1) Yes (2) No	Choose whether or not to reset the policy agent to the default settings.
	QoS Policy Agent Retry Timer (ntnQosConfigQpaRetryTimer)	-1 = no retry, 1..86400	Type the time, in seconds, between the receipt of a connection termination/rejection indication and the start of a new connection request. Note: A value of -1 indicates that a connection retry should not be attempted after a failed attempt.
	Allow Packet Reordering (ntnQosConfigAllowPacket Reordering)	(1) Yes (2) No	Support for certain PHBs requires that packets within a flow not be reordered when transmitted. Choose: • Yes—Allows full flexibility of assigning packet to egress queue. • No—Agent verifies that in-profile and out-of-profile actions associated with the flow do not cause packets from same flow to be assigned to different egress queues.
	Maintain Policing Statistics (ntnQosConfigMaintainPolicing Stats)	(1) Yes (2) No	Policing statistics, such as in-profile and out-of-profile octets, are often important to evaluate the efficacy of the installed policies. Tracking these statistics uses additional system resources, which limits the amount of filters available for classification. Choose: • Yes—Tracks statistics for all policies defined after value is set. • No—Does not track statistics for new policies.
Policy Class Support Table	Policy Class Names		The name of the policy.
	Current Instances		The current class entries.

Table 100 Agent page items (continued)

Section	Item and MIB association	Range	Description
	Maximum Installed Instances		The maximum number of allowed class entries.
Policy Device Identification Table	Description		The system description.
	Maximum Message Size		The maximum target message size supported by the device.

2 In the QoS Configuration section, type information in the text boxes, or select from a list.

3 Click Submit.

Chapter 9
Implementing Common Open Policy Services (COPS)

Enabling COPS in your networks allows the policy server to:

- Gather all relevant information.
- Make a decision based on your (as network administrator) set policies and network resources,
- Communicate that decision in the form of proper service to the appropriate group or client (bandwidth, ACLs, QoS).

A solid COPS strategy is closely tied to Internet Protocol (IP) address management and network management.

This chapter discusses the COPS options available to you in the Web-based management interface.

The COPS options are:

- Viewing COPS statistics and capabilities (next)
- Creating COPS client configurations (page 258)

Viewing COPS statistics and capabilities

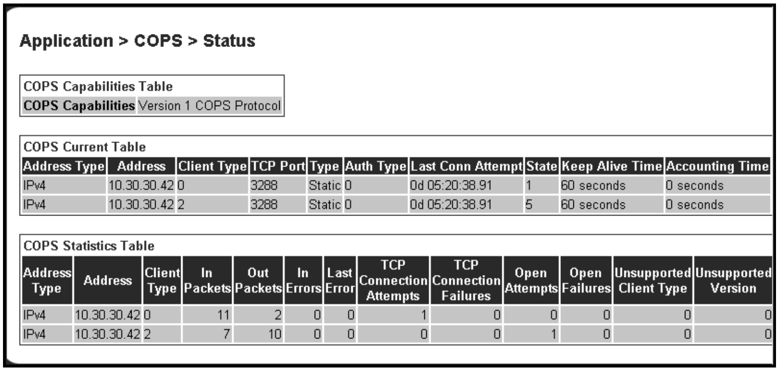
You can view a list of the capabilities of the COPS client to connect to a COPS server and view a table displaying the current status of all COPS server connections.

To view COPS capabilities and statistics:

1 From the main menu, choose Application > COPS > Status.

The Status page opens (Figure 128).

Figure 128 Status page



Application > COPS > Status

COPS Capabilities Table

COPS Capabilities	Version 1 COPS Protocol

COPS Current Table

Address Type	Address	Client Type	TCP Port	Type	Auth Type	Last Conn Attempt	State	Keep Alive Time	Accounting Time
IPv4	10.30.30.42	0	3288	Static	0	0d 05:20:38.91	1	60 seconds	0 seconds
IPv4	10.30.30.42	2	3288	Static	0	0d 05:20:38.91	5	60 seconds	0 seconds

COPS Statistics Table

Address Type	Address	Client Type	In Packets	Out Packets	In Errors	Last Error	TCP Connection Attempts	TCP Connection Failures	Open Attempts	Open Failures	Unsupported Client Type	Unsupported Version
IPv4	10.30.30.42	0	11	2	0	0	1	0	0	0	0	0
IPv4	10.30.30.42	2	7	10	0	0	0	0	1	0	0	0

Table 101 describes the items on the Status page.

Table 101 Status page items

Section	**Item**	**Descriptions**
COPS Capabilities Table	COPS Capabilities	A list of COPS protocols supported by the Business Policy Switch 2000. The current supported version is COPSv1 protocol.
COPS Current Table	Address Type	The type of address in copsClientServerAddress.
	Address	The IPv4, IPv6, or DNS address of a COPS server.
	Client Type	The protocol client type for this entry. Note: Multiple client types can be served by a single COPS server. Note: The value 0 (zero) indicates that this entry contains information about the underlying connection.
	TCP Port	The TCP port number on the COPS server to which the client is connected.

Table 101 Status page items (continued)

Section	Item	Descriptions
COPS Current Table, cont.	Type	The indicator of the source of the COPS server information. Note: COPS servers can be configured by network management into copsClientServerConfigTable and appear in this entry with type copsServerStatic(1). Alternatively, the type, or entry, can be a notification from another COPS server by way of the COPS PDP-Redirect mechanism and appear as copsServerRedirect(2).
	Authorization Type	The indicator of the current security mode in use between the client and the COPS server.
	Last Conn Attempt	The timestamp of the last time the client attempted to connect to this COPS server.
	State	The operational state of the connection and COPS protocol with respect to this COPS server.
	Keep Alive Time	The value of the Keepalive timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates no keepalive activity is expected.
	Accounting Time	The value of the COPS protocol Accounting timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates that the client should not send any unsolicited accounting reports.
COPS Statistics Table	Address Type	The type of address in copsClientServerAddress.
	Address	The IPv4, IPv6, or DNS address of a COPS server.
	Client Type	The protocol client type for this entry. Note: Multiple client types can be served by a single COPS server. Note: The value 0 (zero) indicates that this entry contains information about the underlying connection.
	In Packets	The total number of COPS packets that the client has received from this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Out Packets	The total number of COPS packets that the client has sent to this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	In Errors	The total number of COPS packets that the client has received from this COPS server marked for the selected client type that contained errors in syntax. Note: This is a cumulative value and *is not* zeroed on new connections.
	Last Error	The code contained in the last COPS protocol Error Object received by the client from this COPS server marked for the selected client type. Note: This value *is not* zeroed on COPS Client-Open operations.

Table 101 Status page items (continued)

Section	**Item**	**Descriptions**
COPS Statistics Table, cont.	TCP Connection Attempts	The number of times that the COPS client attempted to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
	TCP Connection Failures	The number of times that the COPS client failed to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
	Open Attempts	The number of times that the COPS client attempted to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Open Failures	The number of times that the COPS client failed to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unsupported Client Type	The total number of COPS packets that this client has received from COPS servers that referred to client types that are unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unsupported Version	The total number of COPS packets that this client has received from COPS servers marked for the selected client type that had a COPS protocol version number that is unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Length Mismatch	The total number of COPS packets that the client received from COPS servers marked for the selected client type that had a COPS protocol message length that did not match the actual received packet. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unknown Opcode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unknown Cnum	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Num not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Bad Ctype	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Type not defined for the C-Nums known by the client. Note: This is a cumulative value and *is not* zeroed on new connections.

Table 101 Status page items (continued)

Section	Item	Descriptions
COPS Statistics Table, cont.	Bad Sends	The total number of COPS packets that the client attempted to send to COPS servers marked for the selected client type that resulted in a transmit error. Note: This is a cumulative value and *is not* zeroed on new connections.
	Wrong Objects	The total number of COPS packets that the client received from COPS servers marked for the selected client type not containing a permitted set of COPS protocol objects. Note: This is a cumulative value and *is not* zeroed on new connections.
	Wrong OpCode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code that should not have been sent to a COPS client, for example, Open-Requests. Note: This is a cumulative value and *is not* zeroed on new connections.
	Timedout Clients	The total number of times that the client has been shut down for the selected client type by COPS servers that detected a COPS protocolKeepalive timeout. Note: This is a cumulative value and *is not* zeroed on new connections.
	Auth Failures	The total number of times that the client received a COPS packet marked for the selected client type that could not be authenticated using the authentication mechanism used by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Auth Missing	The total number of times that the client received a COPS packet marked for this client type not containing authentication information.

Creating a COPS configuration

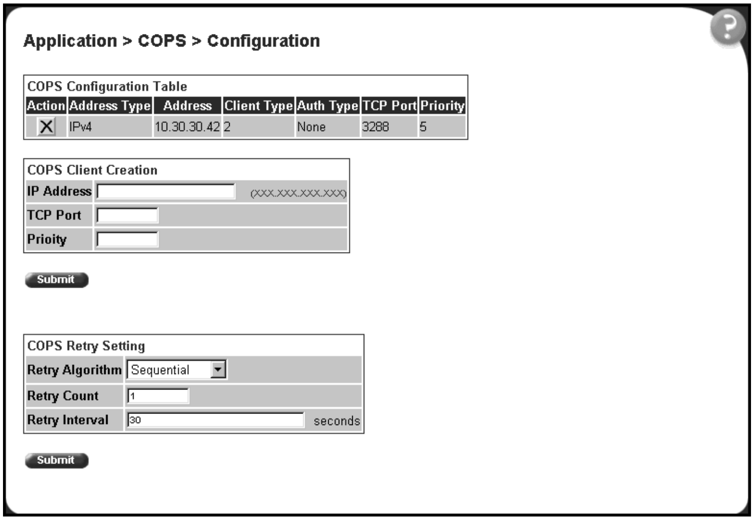
You can select the COPS server(s) to use to obtain policy information by creating COPS configurations.

To create a COPS configuration:

1. From the main menu, choose Application > COPS > Configuration.

   The Configuration page opens (Figure 129).

Figure 129 Configuration page



Application > COPS > Configuration

COPS Configuration Table

Action	Address Type	Address	Client Type	Auth Type	TCP Port	Priority
☒	IPv4	10.30.30.42	2	None	3288	5

COPS Client Creation

IP Address (xxx.xxx.xxx.xxx)
TCP Port
Prioity

COPS Retry Setting

Retry Algorithm: Sequential
Retry Count: 1
Retry Interval: 30 seconds

Table 102 describes the items on the COPS Configuration Table section of the Configuration page.

Table 102 COPS Configuration Table section items

Section	Item	Range	Description
COPS Configuration Table	☒		Deletes the row.
	Address Type		The type of address in copsClientServerConfigAddress.
	Address		The IPv4, IPv6, or DNS address of the COPS server.
	Client Type		The COPS protocol client type this COPS server is capable of serving. Note: A single COPS server can serve multiple client types.

Table 102 COPS Configuration Table section items (continued)

Section	Item	Range	Description
COPS Configuration Table, cont.	Auth Type		The authentication mechanism for this COPS client to request when negotiating security at the start of a connection to a COPS server.
	TCP Port		The TCP port number on the COPS server.
	Priority		The level of priority assigned to the client. Note: When a COPS client attempts to contact COPS servers for the appropriate client type, it contacts higher numbers (priority) first. The order used for server entries with the same priority is undefined. COPS servers notified to the client using the COPS protocol PDP-Redirect mechanism are always processed with higher priority than any entries in this table.
COPS Client Creation	IP Address	XXX.XXX.XXX.XXX	The IP address of the COPS client.
	TCP Port	Integer	Type the TCP port number on the COPS server.
	Priority		Type a number that represents the level of priority. Note: When a COPS client attempts to contact COPS servers for the appropriate client type, it contacts higher numbers (priority) first. The order used for server entries with the same priority is undefined. COPS servers notified to the client using the COPS protocol PDP-Redirect mechanism are always processed with higher priority than any entries in this table.
COPS Retry Setting	Retry Algorithm	(1) Sequential (2) Round Robin	Choose the type of algorithm to use.
	Retry Count	Integer	Type the number of retry attempts.
	Retry Interval	Integer	Type, in seconds, the retry interval.

2 Type information in the text boxes, or select from a list.

Click Submit.

➡ **Note:** COPS configurations are not modifiable. They must be deleted and the information recreated.

Deleting a COPS client configuration

To delete a COPS client configuration:

1. From the main menu, choose Application > COPS > Configuration.

   The Configuration page opens (Figure 129).

2. In the COPS Configuration Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:

   - Click Yes to delete the configuration.
   - Click Cancel to return to the Configuration page without making changes.

Chapter 10
Support menu

The customer support options available to you are:

- Help
- Release Notes
- Manuals
- Upgrade

Using the online help option

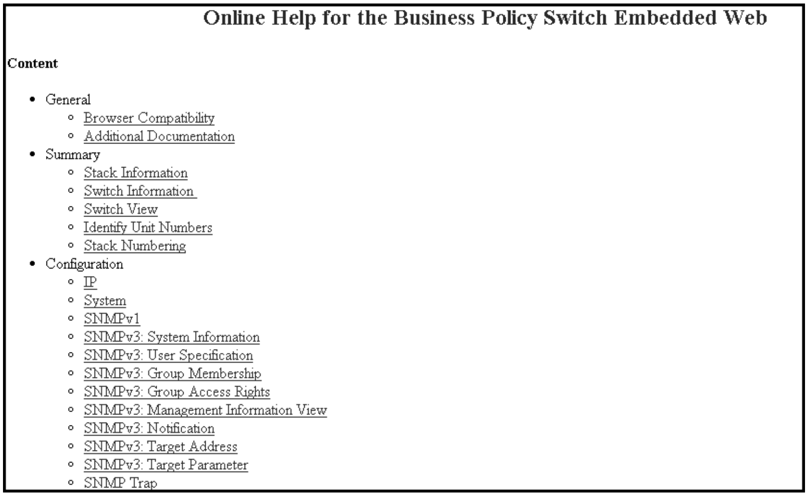
You can read information about management page functions in the online help menu embedded in the Web-based management interface.

To open online help:

1. From the main menu, choose Support > Help or click the Help icon located in the upper right corner of any management page.

   The Online Help menu opens in a separate Web browser (Figure 130).

Figure 130 Online help window



Online Help for the Business Policy Switch Embedded Web

Content

- General
  - Browser Compatibility
  - Additional Documentation
- Summary
  - Stack Information
  - Switch Information
  - Switch View
  - Identify Unit Numbers
  - Stack Numbering
- Configuration
  - IP
  - System
  - SNMPv1
  - SNMPv3: System Information
  - SNMPv3: User Specification
  - SNMPv3: Group Membership
  - SNMPv3: Group Access Rights
  - SNMPv3: Management Information View
  - SNMPv3: Notification
  - SNMPv3: Target Address
  - SNMPv3: Target Parameter
  - SNMP Trap

2 Click on any content item to read information about the topic (if you clicked the Help icon on a management page, information about that page is immediately displayed).

3 Click Return to Top to return to the Content index.

4 Close the Web browser

Downloading technical publications

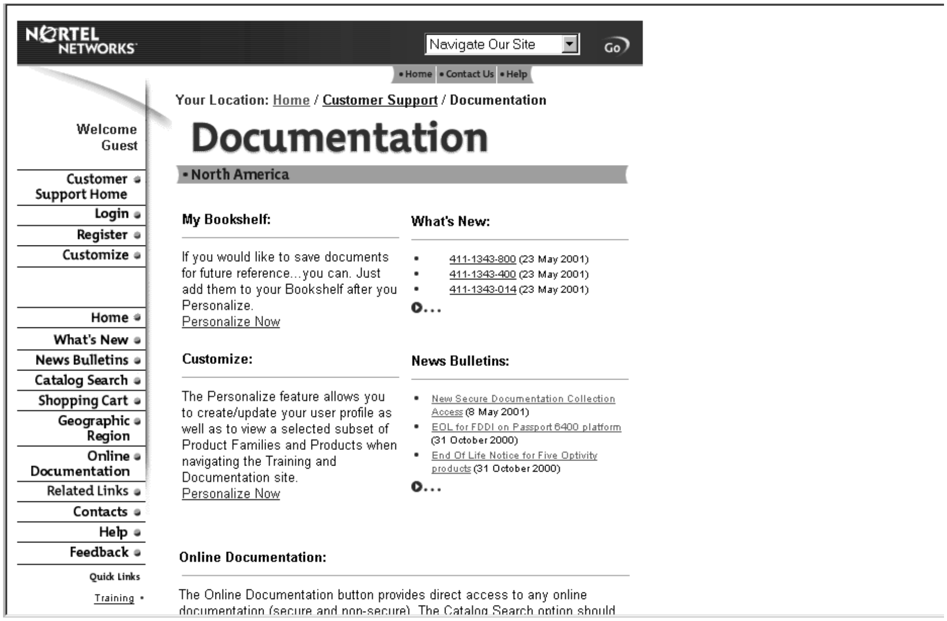
You can download current documentation about the Web-based management user interface from Nortel Networks Technical Documentation Web site.

To download current documentation:

1 From the main menu, choose Support > Release Notes.

Nortel Networks Technical Documentation Web site opens in a separate Web browser (Figure 131).

Figure 131 Nortel Networks Technical Documentation Web site


NORTEL NETWORKS
Navigate Our Site
Go
• Home • Contact Us • Help
Welcome Guest
Customer Support Home
Login
Register
Customize
Home
What's New
News Bulletins
Catalog Search
Shopping Cart
Geographic Region
Online Documentation
Related Links
Contacts
Help
Feedback
Quick Links
Training

Your Location: Home / Customer Support / Documentation

Documentation

• North America

My Bookshelf:

If you would like to save documents for future reference...you can. Just add them to your Bookshelf after you Personalize.
Personalize Now

What's New:

- 411-1343-800 (23 May 2001)
- 411-1343-400 (23 May 2001)
- 411-1343-014 (23 May 2001)

Customize:

The Personalize feature allows you to create/update your user profile as well as to view a selected subset of Product Families and Products when navigating the Training and Documentation site.
Personalize Now

News Bulletins:

- New Secure Documentation Collection Access (8 May 2001)
- EOL for FDDI on Passport 6400 platform (31 October 2000)
- End Of Life Notice for Five Optivity products (31 October 2000)

Online Documentation:

The Online Documentation button provides direct access to any online documentation (secure and non-secure). The Catalog Search option should

2 Locate your product, and click the document you want to download.

The BPS 2000 documentation is in the Data and Internet Product Family.

3 Click on the PDF icon to start the download process (you need Adobe Acrobat 3.0 or later to view or print documents from this site).

4 Follow the prompts to download the documentation.

5 Close the Web browser.

Upgrade option

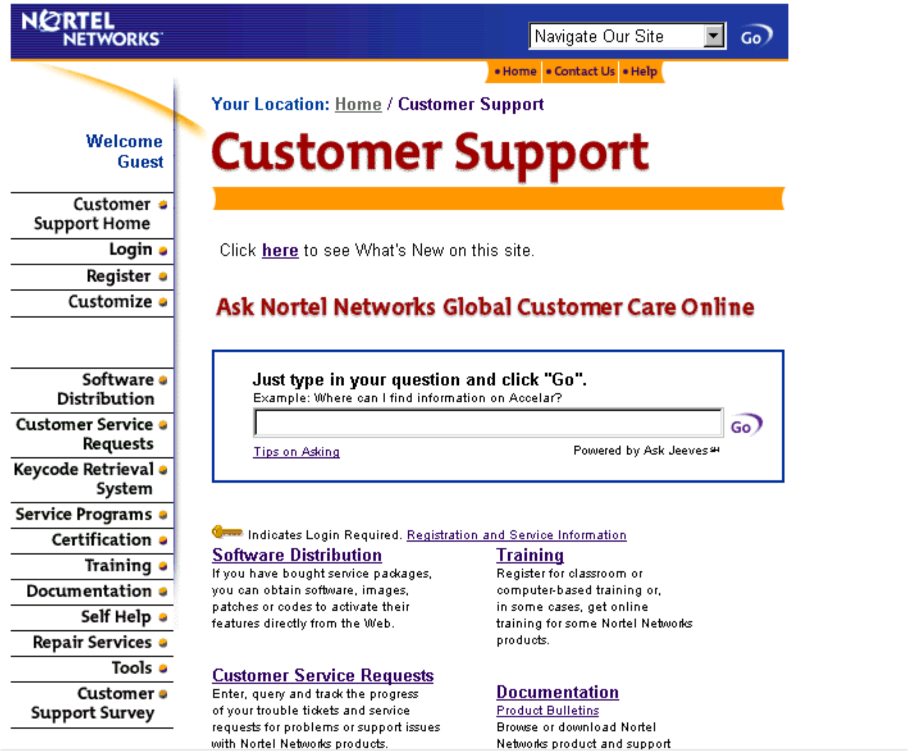
You can upgrade your Web-based management user interface to the most recent software release.

To upgrade to the most recent software release:

1 From the main menu, choose Support > Upgrade.

Nortel Networks Customer Support opens in a separate Web browser (Figure 132).

Figure 132 Nortel Networks Customer Support Web site


NORTEL NETWORKS
Navigate Our Site
Go
• Home • Contact Us • Help
Welcome Guest
Customer Support Home
Login
Register
Customize
Software Distribution
Customer Service Requests
Keycode Retrieval System
Service Programs
Certification
Training
Documentation
Self Help
Repair Services
Tools
Customer Support Survey
Go
Tips on Asking
Powered by Ask Jeeves℠

Your Location: Home / Customer Support

Customer Support

Click here to see What's New on this site.

Ask Nortel Networks Global Customer Care Online

Just type in your question and click "Go".
Example: Where can I find information on Accelar?

Indicates Login Required. Registration and Service Information

Software Distribution
If you have bought service packages, you can obtain software, images, patches or codes to activate their features directly from the Web.

Training
Register for classroom or computer-based training or, in some cases, get online training for some Nortel Networks products.

Customer Service Requests
Enter, query and track the progress of your trouble tickets and service requests for problems or support issues with Nortel Networks products.

Documentation
Product Bulletins
Browse or download Nortel Networks product and support

2 Follow the prompts to download the software release.

3 Close the Web browser.

Index

Numbers

450 Image Filename field 106

802.1p Assignment Table 212

802.1p Priority field 211, 213, 216, 229, 234, 236

802.1p Priority Mapping page 212

802.1p Priority Queue Assignment page 211

A

Absolute Bandwidth field 205

access 87
- console 111
- MAC address-based 89
- number 43
- RADIUS security 42
- SNMP 87, 90
- Telnet 87
- TELNET/WEB/SNMP 25
- user levels 43
- Web 29

Accounting Time field 255

Action Creation 237

Action Name field 238

Action page 237

Action Table 237

Active Phy field 105

Address Type field 258

administrative options
- logging on 42
- logging out 45
- resetting the switch/stack 43
- resetting to system defaults 44
- security, configuring
  - passwords 39
  - remote dial-in access 41
- system information, viewing 38

Administrative Status field 86

Administrative Traffic Control field 86

Agent page 249

Aging Time field 100

alarms 114, 117

Alignment Errors field 138

Allow Packet Reordering field 250

Allowed Source field 95

Allowed Source IP field 89

Allowed Source Mask field 89

application setting options
- broadcast domains 172
- Common Open Policy Services (COPS) 254
- IGMP 151
- MultiLink Trunking 186
- port mirroring 146
- QoS 212
  - 802.1p priority queue assignment 210
  - DSCP mapping 215
  - DSCP queue assignment 213
  - interface groups 204
  - layer 2 filters 227
  - network access 218
  - policies (hardware filters) 244
  - Policy Agent (QPA) 248
  - role combination 204
- rate limiting 149
- VLANs 157

Auth 257

Auth Failures field 257

Auth Missing ffield 257

Auth Type field 259

Authentication Password field 67

Authentication Protocol field 66

Authentication Protocols Supported field 64

Authentication Trap field 63

authentication traps, enabling 62

Authorization Type field 255

Autonegotiation field 103, 105

autonegotiation, configuring 102

autoPVID 25, 156, 172, 174

AutoPVID field 158

AutoTopology field 63

Autotopology, enabling 62

B

Bad Ctype field 256

Bad Sends field 257

Bandwidth Allocation field 205

Bandwidth field 205

bandwidth utilization 189, 205

BaySecure 89

BootP
  configuring 58

bootP
  request modes 59

BootP Request Mode field 59

BPS 2000 Diagnostics Filename field 106

BPS 2000 Image Filename field 106

Bridge Forward Delay field 185

Bridge Hello Time field 185

Bridge Information page 183

Bridge Maximum Age Time field 185

Bridge Priority field 177, 184

bridge settings 183

broadcast domains, configuring 172

Broadcast field 121, 125, 129

broadcast traffic 149

C

Capabilities field 209

Carrier Sense Errors field 138

Cascade Ports field 209

check boxes, about 34

Clear by Ports page 97

Clear Message From field 119

Client Type field 254, 258

Collisions field 121, 130

Comm Port Data Bits field 111

Comm Port Parity field 111

Comm Port Stop Bits field 111

Committed Burst Size field 242, 243

Committed Rate field 242, 243

Common Open Policy Services (COPS)
  sequential algorithm 259

Common Open Policy Services (COPS)
  about 253
  configuring 257
  deleting a client 260
  round robin algorithm 259
  statistics 255
  viewing capabilities and statistics 254

Community field 83

community strings, configuring 62

configuration file 108, 110

Configuration File Download/Upload page 108

Configuration Image Filename field 109

Configuration page 257

Console page 34, 39

Console Password Setting page 39

Console Port Speed field 111

Console Stack Password Type field 40

Console Switch Password Type field 40

Console/Communication Port page 111

conventions, text 22

conversation steering 146

COPS Capabilities field 254

Copy Configuration Image to Server field 109

CRC Align Errors field 121, 125

Current Learning Mode field 91

Current Level field 115

Current Running Version field 106

customer support 23

D

DA Filtering on Intrusion Detected field 91

Data Specification field 242, 243

Decryption Error field 65

Default Gateway field 59

default mapping 210, 212, 213, 215

default settings 44

Deferred Packets field 130

Deferred Transmissions field 139

Description field 48

Designated Root field 184

Destination Address field 220, 224, 225

Destination Address Mask field 220, 224, 225

Destination IP L4 Port Max field 230

Destination IP L4 Port Min field 230

Destination IP L4 Port Range field 232

Destination L4 Port field 220, 224, 225

Destination L4 Port Max field 234, 236

Destination L4 Port Min field 234, 236

Display Message From field 119

Display Unit field 119

Download Option field 106

Drop 125

Drop Events field 120, 125

drop precedence 215

Drop Precedence field 216, 217

DSCP 225
- 802.1p priority mapping 215
- QoS
  - mapping 212
- queue set associations 213

DSCP field 213, 214, 216, 220, 221, 224, 225, 229, 234, 236

DSCP Mapping Modification page 215

DSCP Mapping page 215

DSCP Queue Assignment page 214

E

EAPOL Administrative State field 86

EAPOL Security Configuration page 84

EAPOL-based network security 25

EAPOL-based security 25, 84

Entry field 93, 95

Entry Storage field 66, 69, 72, 74, 76, 79, 81, 206

errors 132, 134, 137, 141

Ethernet error statistics
- viewing 137
- viewing in a bar graph format 140
- viewing in a pie chart format 139

Ethernet Errors
- Chart page 139

Ethernet Errors page 137

EtherType field 229, 234, 236

Excessive Collisions field 130, 133, 139

Extended Discipline field 205

F

fault threshold parameters, configuring 114

FCS Errors field 129, 133, 138

features 25

Filter Group field 246, 247
Filter Group Name field 224, 225, 234, 236
Filter Group Type 247
Filter Group Type field 246
Filter Tagged Frames field 173
Filter Unregistered Frames 173
Filter Untagged Frames field 173
Filtererd Packets field 129
Find MAC Address page 100
Flooded Packets field 129
Flow Control field 105
Forward Delay field 185
Forward Delay Time field 178
Fragments field 121
Frame Errors field 129, 133
Frame Too Long field 138

G

gateway addresses, configuring 58
GBIC 25
General Discipline field 205
Generate SNMP Trap on Intrusion field 91
gigabit Ethernet 25, 104
Group Access Rights page 71
Group Creation page 177
Group Membership page 68
Group Name field 69, 72
Group page 186
Group Setting page 180

H

hardware description 48, 50
Hello Interval 178
Hello Time field 178, 184
High Speed Flow Control page 104
high speed flow control, configuring 104
Host Address field 221
Hybrid Stack 112
hybrid stack 27

I

icons, about 34
Identify Unit Numbers page 56
IGMP Multicast Group Membership page 154
IGMP page 151
IGMP VLAN Configuration page 152
IGMP, configuring 151
In Discards field 135, 142
In Errors field 135, 255
In Frames field 142
In Non-Unicast field 135
In Octets field 135
In Packets field 255
In Unicast field 135
In Unknown Protos field 135
In-Band Stack IP Address field 59
In-Band Subnet Mask field 59
In-Band Switch IP Address field 59
Initialize field 86
In-Profile Action field 242, 243
In-Profile Octets field 248
Interface
    Chart page 136
Interface chart field 135
interface class
    trusted, untrusted, and unrestricted 206, 209, 217
Interface Class field 206, 209
Interface Configuration page 204
Interface Direction field 246
Interface Group Assignment page 208

Interface Group Creation 204

Interface Group Table 204

Interface ID page 207

Interface ID Table 207

Interface page 134

Interface Queue Table 204

interface statistics
- viewing 134, 135
- viewing in a bar graph format 136
- viewing in a pie chart format 136

Internal MAC Receive Errors field 138

Internal MAC Transmit Errors field 138

Interval field 116

In-Use field 59

IP address 58

IP Address field 48, 50, 83, 199, 259

IP Classification Group page 222, 223

IP Classification page 218

IP Filter Creation 218

IP Filter Group Table 218

IP Filter Table 218

IP gateway address 58

IP Group Modification page 224

IP manager list 25, 87

IP manager-based network security 25

IP page 58

IP Protocol field 199, 230

J

Jabbers field 121

K

Keep Alive Time field 255

L

L4 Port Dst field 199

L4 Port Src field 200

Last BootP field 59

Last Conn Attempt field 255

Last Error field 255

Late Collisions field 130, 133, 139

Layer2 Classification page 227

Layer2 Filter Creation 227

Layer2 Filter Group Table 227

Layer2 Group modification page 235

Layer2 Group page 233

Layer2Filter Table 227

Learn by Ports page 93

Learning Constraint field 158, 159, 161, 163, 167, 168, 170

LEDs 43, 44, 51, 56

Length Mismatch field 256

Limit field 150

Link field 103, 133

Link/Trap field 103

Local Store Version field 106

logging on 42

logging out 45

Lost Packets field 129

M

MAC address 50

MAC Address field 48, 55, 95, 100

Mac Address field 50

MAC Address page 170

MAC address security 90
- allowed source 94
- clearing 97
- deleting ports 98
- learn by ports 93
- learning 91
- ports 97
- security list 92

  security table 94
MAC Address Security field 91
MAC Address Security SNMP-Locked field 91
MAC Address Table page 99
MAC address-based port mirroring 146, 148
MAC addresses
  locating a specific address 100
  viewing learned addresses 99
main menu
  headings and options 32
  icons 33, 35
Maintain Policing Statistics field 250
Maks Bit field 199
Management Information View page 73
Management VLAN field 158
Manufacturing Date Code field 48, 50
Max. Age Time field 178
Maximum Age Time field 185
Maximum Installed Instances filed 251
Maximum Message Size field 251
Maximum Requests field 86
MDA Description field 50
MDA field 48
MDAs 25, 104
Message field 119
Message Type field 119
Meter Creation 241
Meter field 246
Meter page 241
Meter Table 241
Meters page 243
Microsoft Internet Explorer, software version requirements 28
mixed stack 26, 27
Module Description field 50
Monitor Port field 147
Monitoring 147
Monitoring Mode field 147
monitoring modes 148
Msg Processing Model field 81
multicast 151
Multicast field 121, 125, 129
Multicast Group Address field 154
multicast traffic 149
MultiLink Trunking 182
  about 186
  configuring 186
  monitoring traffic 189
Multiple Collision Frames field 139
Multiple Collisions field 130, 133
multiple spanning tree groups 25, 176

N

Netscape Navigator, software version requirements 28
network access, configuring IP filters 217
Network Addres field 220
network administrator
  contact information 60, 61
network monitoring 113
network security, protecting system integrity 30
new features 25
New Unit Number field 55
Not in Time Window field 65
Notification page 76
Notify Name field 76
Notify Tag field 76
Notify Type field 76
Notify View field 72
numbering
  ports 29
  stacks 54
  unit 29, 50, 54, 56

O

Octets field 120, 125
online help, accessing 261
Open Attempts field 256
Open Failures field 256
Operational State field 48, 50
Operational Status field 86
Operational Traffic Control field 86
Order field 224, 225, 234, 236
Out Discards field 135
Out Errors field 135
Out Frames field 142
Out Non-Unicast field 135
Out Octets field 135
Out Packets field 255
Out Profile field 248
Out Unicast field 135
Out-Profile Action field 243
Out-Profile action field 242
Overflow Packet Hits field 247
Oversize field 121, 125
Oversized Packets field 129

P

Packet Hits field 247
Packet Type field 150
Packets field 121, 125, 129
Packets length field 121, 129
Parameter field 115
Parameter Tag field 81
Participation field 182
Partition Port on Intrusion Detected field 91
Partition Time field 91
passwords, setting
  console 39
  remote dial-in access 41
  Telnet 39
  Web 39
Path Cost field 183
Permit field 220, 224, 226
physical view 51
PIDs 164
Policies page 244
Policy Class Name field 250
Policy Name field 246, 247
Policy Order field 246
Policy Statistics page 247
Port
  Chart page 131
port autonegotiation speed, configuring 102
Port Based modification page 160
Port Based page 159
port communication speed, configuring 111
Port Configuration page 97, 172, 181
Port Error Summary page 132
Port Information page 174
port list 29
Port List field 91, 93
Port List page 93
Port Lists page 92
Port Management page 102
Port Membership field 209
port mirroring 146
Port Mirroring page 146
Port Name field 173
port number 29
Port page 127
Port Priority field 174
port statistics 26
  viewing 127, 128, 132
  viewing in a bar graph format 131

- viewing in a pie chart format 131
- zeroing ports 130

Port/Port Membership field 161, 167

port-based port mirroring 146, 148

ports
- enabling 103
- trusted, untrusted, and unrestricted 206, 217

power status 49

Power Status field 50

Preconfigured Port # field 221

Preferred Phy field 105

Primary RADIUS Server field 41

Priority field 182, 259

Private Protocol field 66

Private Protocols Supported field 64

product support 23

Protocol field 158, 163, 220, 221, 224, 225, 234, 236

Proxy field 151, 153

publications
- hard copy 23
- related 22

Pure BPS 2000 Stack 112

PVID 25, 172

PVID field 174, 175

Q

QoS 210, 212, 213, 215
- 802.1p priority mapping, configuring 212
- 802.1p priority, configuring 210
- about 192
- actions 237
- bandwidth allocation 205
- burst size 241
- capabilities 206
- committed rate 241
- COPS 248, 253, 254
- data specification 241
- defined filters, installing 241, 244
- discipline 205
- drop precedence 215
- DSCP
  - queue set association, creating 213
- DSCP mapping
  - configuring 215
- duration 241
- entry storage 206
- Ethertype 227
- filter actions
  - about 237
  - deleting 240
- hardware filters
  - deleting 248
  - installing 244
  - viewing statistics 247
- ignore vlaue 219
- in-profile action 239
- interface class (trusted, untrusted, unrestricted) 206, 217
- Interface Configuration page 204
- Interface Group Assignment page 208
- interface groups 204
  - configuring 204
  - deleting 210
  - modifying 207
- IP filter groups
  - about 217
  - configuring 222
  - deleting 226
  - modifying 224
- IP filters
  - about 217
  - configuring 217
  - deleting 222
- layer 2 filter groups
  - about 227
  - configuring 233
  - deleting 236
  - modifying 235
- layer 2 filters
  - about 227
  - creating 227
  - deleting 232

loss sensitivity 217, 237
matching 217, 227
metered data 239
metering 25
meters 239
  deleting 243
no meter data 239
order 222
out-of-profile action 239
packet reordering 244, 248
policies 204
  configuring 241, 244
  statistics 247
policing 25
policy server control 248
ports 204
  adding or removing 208
  type (trusted, untrusted, unrestricted) 206
  type (trusted, untrusted, untrestricted) 217
queue sets 210, 211, 213, 250
  DSCP associations, creating 213
role combinations
  adding 208
  deleting 210
  modifying 207
  removing 208
sample using Advanced pages 204
sample using Wizard 192
service order 205
statistics 244, 246, 247, 248, 250
tagging 229, 230, 234
traffic flows 203
traffic policing 239, 241
trusted ports 206, 217
unrestricted ports 206, 217
untrusted ports 206, 217
VLAN tagging 227
Web-based QoS Wizard
  about 192
Wizard
  classifying traffic 198
  prioritizing traffic 195
  prioritizing VLANs 201
  standard traffic 192
  traffic flows 198
QoS Policy Agent Reset to Defaults field 250
QoS Policy Agent Retry Timer field 250
QoS Policy Agent State 250
QoS policy agent, configuring 248
QoS Policy Server Control field 250
Query Time field 152, 153
Queue field 211, 214
Queue Set field 211, 214
Queue Sets field 208
Quiet Period field 86

R

RADIUS page 41
RADIUS Shared Secret field 41
RADIUS-based network security 41, 84
rate limiting
  about 149
  configuring 149
Rate Limiting page 149
Read View field 72
Read-Only Community String field 63
Read-Only Stack Password field 40
Read-Only Switch Password field 40
Read-Write Community String field 63
Read-Write Stack Password field 40
Read-Write Switch Password field 40
Re-authenticate Now field 86
Re-authentication field 86
Re-authentication Period field 86
redundancy 186
Remote Access page 87
remote dial-in access, configuring 41
Reset page 44
Reset to Defaults page 45
resetting the switch/stack 43

resetting the switch/stack, to system defaults 44

Retrieve Configuration Image from Server field 109

Retry Algorithm field 259

Retry Count field 259

Retry Interval field 259

Rising Action 115

Rising Level field 115

RMON
- Ethernet statistics
  - viewing 120
  - viewing in a bar graph format 122
  - viewing in a pie chart format 123
- history statistics
  - viewing 124
  - viewing in a line graph format 126

RMON Ethernet
- Chart page 122

RMON Ethernet page 120

RMON Event Log page 117

RMON History
- Chart page 126

RMON History page 124

RMON options
- fault event log, viewing 117
- fault threshold parameters
  - configuring 114
  - deleting 116
- history statistics
  - viewing 124

RMON Threshold Creation field 116

RMON Threshold page 114

RMON, about 113

Robust Value field 152, 153

Role Combination field 206, 208, 209, 246, 247

role combinations 204

Root Path Cost field 184

Root Port field 184

S

Sample/Alarm Sample field 116

Secondary RADIUS Server field 41

security 25, 84
- EAPOL-based 25
- IP manager list 25
- MAC address-based 90
- passwords 39
- RADIUS-based 41
- remote dial-in access 41
- SNMPv3 61, 63

Security Configuration page 90

Security field 98

Security Level field 72, 81

Security Model field 69, 72

Security Name field 69, 81

Security page 90

Security Table page 94

Select VLANs field 100

Serial Number field 48, 50

Server Timeout field 86

Service Class field 216, 217

Service Order field 205

Set Drop Precedence field 239

Single Collision Frame field 139

Single Collisions field 130

SNMP
- about 61
- MAC address security 91
- trap receivers
  - configuring 82
  - deleting 83

SNMP Engine Boot field 64

SNMP Engine Dialect field 64

SNMP Engine ID field 64

SNMP Engine Maximum Message Size field 64

SNMP Engine Time field 64

SNMP Trap Receiver page 82

SNMP/Access field 88

SNMP/Use List field 88

SNMPv1
- about 61
- configuring 62

SNMPv1 page 62

SNMPv3 63
- about 61
- configuring 63
- group access rights 71
  - deleting 72
- group membership 68
  - deleting 70
- management information views 73
  - deleting 75
- system information, viewing 63
- system notification entries 75
  - deleting 77
- target addresses 78
  - deleting 80
- target parameters 80
  - deleting 82
- user access 65
  - deleting 68

Snooping field 151, 152

software download
- LED indication descriptions 107
- process 105, 107

Software Download page 106

software upgrade 25, 263

Software Version field 48, 50

software version requirements
- Microsoft Internet Explorer 28
- Netscape Navigator 28

software versions 25, 26, 27, 39, 47, 106

Source Address field 220, 224, 225

Source Address Mask field 220, 224, 225

Source field 100

Source IP L4 Port Max field 230

Source IP L4 Port Min field 230

Source IP L4 Port Range field 232

Source L4 Port field 220, 224, 226

Source L4 Port Max field 235, 236

Source L4 Port Min field 234, 236

spanning tree 176
- bridge information 183
- learning mode 188
- learning modes 182

Spanning Tree Add VLAN page 178

spanning tree configuration 181

spanning tree groups 25, 176
- adding VLANs 178
- bridge information 183
- configuring 177
- default 176
- number of 26, 28
- ports 181
- removing VLANs 178
- tagging 176, 178, 180
- VLANs 178

spanning tree ports
- configuring 181
- enabling 181
- FastLearning 181

Speed/Duplex field 103, 133

SQE Test Errors field 139

Stack Information page 47

stack information, viewing 47

Stack Numbering page 54

stack numbering, configuring 54

stack operational mode 44

Stack Operational Mode page 112

stack operational modes 112

stacking 26, 27, 44, 47, 54, 112, 155

Start field 125

State field 158, 183

Static Router Ports field 153

statistics 26, 113, 122, 124, 126, 127, 130, 132, 137, 141

Status field 133

Status page 254

STGs 176

STP Learning field 188

Subnet Mask field 220

summary options
  changing stack numbering 54
  identifying unit numbers 56
  viewing
    stack information 47
    switch information 49
    switch information in real time 51

Supplicant Timeout field 86

Support menu
  online help 261
  technical publications 262
  user interface, upgrading 263

support, Nortel Networks 23

switch configuration files
  requirements for retrieving 110
  requirements for storing 110
  TFTP server 108

switch images, downloading 105

switch information
  viewing 49
  viewing in real-time 51

Switch Information page 49

Switch View page 51

sysContact field 39

sysDescription field 39

sysLocation field 39

sysName field 39

System Contact field 61

system default settings, resetting to 44

System Description field 48, 61

System Information page 38, 42, 63

system information, viewing 38

System Location field 61

system location, naming 60

System Log page 118

system log, viewing 118

System Name field 61

system name, configuring 60

System Object ID field 61

system operational modes, configuring 112

System page 60

system settings
  modifying 60
  system contact 61
  system location 61
  system name 61

system statistics options, viewing
  Ethernet error statistics 137
  interface statistics 134
  port statistics 127
  QoS 247
  transparent bridging statistics 141

System Up Time field 61

sysUpTime field 39

T

tables and input forms, about 34

Tagged BPDU on Tagged Port field 178

tagged frames 172

Tagged Trunk 174

tagged trunk 161

tagging 161, 172, 182

Tagging field 174, 182

Target Address field 79

Target Address page 78

Target Domain field 79

Target Name field 79

Target Parameter Entry field 79

Target Parameter page 80

Target Retry Count field 79

Target Tag List field 79

Target Timeout field 79

TCP 199

TCP Connection Attmepts field 256

TCP Connection Failures field 256

TCP Port field 254, 259

technical publications 23, 262

technical support 23

Telnet Password Setting page 39

Telnet/Access field 88

Telnet/Use List field 88

text conventions 22

TFTP
- configuration file 108
- server 108
- software download 108

TFTP Server IP Address field 106, 109

Time Stamp field 118, 119

Timeout Clients field 257

Total Octets field 129, 247

Total Overflow in Profile Octets field 248

Total Overflow Octets field 247

Total Overflow Out Profile Octets field 248

Track Statistics field 246

traffic policing 241

Traffic Type field 189

traffic, classifying 217

Transmit Period field 86

Transmit/Drop Frame field 238

Transparent Bridging
- Chart page 143

Transparent Bridging page 141

transparent bridging statistics
- viewing 141, 142
- viewing in a bar graph format 144
- viewing in a pie chart format 143

Trap Receiver Index field 83

traps 82

Triggered By field 118

troubleshooting 26
- access 87, 89
- configuration file 110
- COPS 259
- defaults 44
- mixed stack 27
- QoS 192, 204, 206, 210, 212, 213, 215, 217, 239, 241, 245
- spanning tree groups 28, 176, 180
- stacking 26, 53, 112
- STGs 176
- VLANs 28, 155, 158, 162, 172, 180

Trunk field 182

Trunk Mode field 188

Trunk Name field 188

Trunk Port Members field 188

Trunk Status field 188

trusted ports 206, 209, 217

U

UDP 199

UDP RADIUS Port field 41

Unavailable Context field 65

Undersize field 121, 125

Undersized Packets field 129

Unit field 48, 50

unit number 29, 50, 54

unit numbers
- identifying 56

unit numbes
- numbering
  - units 48

Unknown Context field 65

Unknown Ctype field 256
Unknown Engine IDs field 65
Unknown Opcode field 256
Unknown User Name field 65
unregistererd frames 172
unrestricted ports 206, 209, 217
Unsupported Client Type field 256
Unsupported Security Level field 65
Unsupported Version field 256
Untagged Access 174
untagged access 161
untagged frames 172
untrusted ports 206, 209, 217
Update 802.1p Priority field 239
Update DSCP field 238
upgrades 25
User Defined Port # field 221
User Defined Protocol field 158, 163
user interface, upgrading 263
User Name field 66
User Specification page 65
Utilization page 189

V

View Mask field 74
View Name field 74
View Subtree field 74
View Type field 74
VLAN Configuration
  MAC SA Based modification page 169
  MAC SA Based setting page 167
  Protocol Based modification page 166
  Protocol Based setting page 162
VLAN Configuration page 157
VLAN field 236
VLAN Membership
  Add VLAN page 179
  Remove VLAN page 180
VLAN Membership page 179
VLAN Name field 158, 159, 163, 167, 168, 170, 175
VLAN Tag field 229, 230
VLAN Tag Required field 234, 236
VLAN Type field 158, 175
VLANs 25, 155
  about 155
  autoPVID 156, 158
  broadcast domains, configuring 172
  configuring 157
  deleting 172
  finding MAC addresses 100
  learned MAC addresses 99
  MAC SA-based
    about 156
    assigning MAC addresses 170
    configuring 167, 171
    deleting MAC addresses 171
  mixed stack 155
  number of 25, 26, 28, 155
  port information
    viewing 174
  port-based
    about 156
    configuring 159
  protocol-based
    about 156
    configuring 162
    number of 156
    number of protocols 162
    reserved PID types 165
    supported PID types 164
  selecting a management VLAN 171
  STG 27
  tagging 229, 230, 234

W

Web browser, requirements 28

Web Page/Access field 88

Web Password Setting page 39

Web/Use List field 89

Web-based management interface
  home page, graphic 30
  logging in 29
  main menu, icons 33, 35
  management page 34
  navigating the menu 31
  requirements to use 28
  Web page layout 30
  Web page layout, graphic 31

Write View field 72

Wrong Digest field 65

Wrong Objects field 257

Wrong OpCode field 257